UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

TRABAJO DE GRADO:

"DESAFÍOS DEL SISTEMA PENAL SALVADOREÑO EN LA APLICACIÓN DE LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS".

PRESENTADO POR:

MARTÍNEZ SERPAS MARÍA JOSÉ

MURILLO MEDINA HELEN ELIZABETH

SÁNCHEZ VENTURA ESTEPHANI GABRIELA

PARA OPTAR AL GRADO ACADÉMICO DE:

LICENCIADAS EN CIENCIAS JURÍDICAS

DOCENTE ASESOR:

MSC. ROSA YANETH PINEDA DE IGLESIAS

SAN MIGUEL, EL SALVADOR, C.A. CIUDAD UNIVERSITARIA DE ORIENTE, AGOSTO DE 2020.

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES

MSC. ROGER ARMANDO ARIAS ALVARADO.
RECTOR.

DR. RAÚL ERNESTO AZCÚNAGA LÓPEZ.
VICERRECTOR ACADÉMICO.

ING. JUAN ROSA QUINTANILLA QUINTANILLA.
VICERRECTOR ADMINISTRATIVO.

ING. FRANCISCO ANTONIO ALARCON SANDOVAL.
SECRETARIO GENERAL.

LIC. RAFAEL HUMBERTO PEÑA MARÍN.
FISCAL GENERAL.

FACULTAD MULTIDISCIPLINARIA ORIENTAL

AUTORIDADES

LIC. CRISTÓBAL HERNÁN RÍOS BENÍTEZ.

DECANO.

LIC. OSCAR VILLALOBOS.

VICE-DECANO.

LIC. ISRAEL LÓPEZ MIRANDA.

SECRETARIO INTERINO.

LIC. JORGE PASTOR FUENTES CABRERA.

DIRECTOR GENERAL DE PROCESOS DE GRADUACIÓN DE LA FACULTAD.

DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES

AUTORIDADES

LIC. JOSÉ PEDRO CRUZ CRUZ.

JEFE DEL DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

LIC. JOSÉ PEDRO CRUZ CRUZ.

COORDINADOR DE PROCESOS DE GRADUACIÓN EN FUNCIONES DEL DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

MSC. ROSA YANETH PINEDA DE IGLESIAS.

ASESOR DE CONTENIDO.

LIC. CARLOS ARMANDO SARAVIA SEGOVIA.

ASESOR DE METODOLOGIA.

DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

TRIBUNAL EVALUADOR.

LIC. ANTONIO ENRIQUE ARGUETA NOLASCO

PRESIDENTE

MSC. HUGO NOÉ GARCÍA GUEVARA

SECRETARIO

MSC. ROSA YANETH PINEDA DE IGLESIAS

VOCAL

AGRADECIMIENTOS.

Han sido tantas las personas que han contribuido en el proceso y finalización de este trabajo. En primer lugar, quiero agradecer a Dios, mi héroe número uno, por haberme brindado la fortaleza para culminar con mis estudios, por llenarme de sabiduría en momentos en los que todo parecía oscuro y nunca soltar mi mano, porque fue Él quien me sostuvo y siempre me sostendrá. Infinitas gracias padre Celestial.

A mi familia, especialmente a mis héroes aquí en la tierra, mi padre Fernando Arnoldo Martínez por ser el principal promotor de mis sueños, el pilar fundamental de mi vida, quien con su amor, dedicación y apoyo me ha formado, gracias por creer siempre en mí, a José Gilberto Rosa por mostrarme su amor y nunca dejarme sola cuando más lo necesite, a mi madre Vilma Dinora Serpas por siempre cuidar de mí y ayudarme en todo momento, a mis hermanas Karla y Evelyn Martínez por animarme a seguir cuando ya no quería y a mis sobrinos por ser mi luz.

A mis amigos, especialmente a mi gran y mejor amiga, mi hermana de corazón Jeannette Zelaya por siempre creer en mi más de lo que yo misma creía en ocasiones, por tu ayuda desinteresada a lo largo de mi vida y por estar conmigo en las buenas, en las malas y peores. Sos luz en mi vida, gracias infinitas.

A mis amigas, compañeras de luchas, quienes me acompañaron y ayudaron durante todo el proceso, con quienes compartí noches de desvelo, preocupaciones y al mismo tiempo alegrías y risas, gracias totales por nunca dejarme sola.

A mis compañeras de tesis, Estephani y Helen, quienes han sido mis mejores amigas y mis confidentes, gracias por todas las experiencias vividas

a lo largo de nuestra carrera, por confiar en mí y tenerme la paciencia necesaria, apoyarme y motivarme a seguir adelante en los momentos de desesperación, tienen un lugar demasiado grande en mí.

A nuestros asesores, especialmente a nuestra asesora de contenido Jeaneth Pineda por guiarnos en este proceso y ayudarnos a culminar nuestra carrera, así mismo a todos los docentes y demás asesores por su ayuda desinteresada al compartirnos sus conocimientos.

Definitivamente no ha sido sencillo el camino hasta aquí, pero gracias a sus aportes, su amor, amistad, apoyo e inmensa bondad el camino fue más liviano, les agradezco demasiado y expreso mi afecto hacia todos ustedes.

Martínez Serpas María José

AGRADECIMIENTOS

Doy gracias a Dios por haberme permitido culminar mis estudios y cuidar de mí a lo largo de esta carrera por darme paciencia para no rendirme.

A mi padre, que de alguna manera estuvo presente durante todo este tiempo.

A mi tía, que a pesar de la distancia me ha brindado su apoyo y su ayuda.

A mi madre y mis hermanos por estar presente en todas circunstancias de mi vida, por el apoyo incondicional que me brindan siempre.

A mis amigas que hice a lo larga de esta carrera, a cada una de ellas que formaron parte de esta aventura universitaria gracias por haber sido un apoyo para no rendir.

A ti Mauricio que en estos últimos años me has ayudado a seguir adelante y poder culminar la carrera, y a mis pequeños hijos que fueron mi motor para poder seguir.

A MIS AMIGAS y compañeras de tesis por la paciencia, por esas noches desvelo y mucha tolerancia realmente gracias…

Murillo Medina Helen Elizabeth

AGRADECIMIENTOS

Le doy gracias a Dios por permitirme llegar hasta aquí, porque TODO se lo debo a él, por haberme dado la capacidad, la fortaleza y guiarme siempre. Y porque sé que lo seguirá haciendo en todo el trayecto de mi vida.

A mis papas Karla y Julio, por ser mi apoyo incondicional en todo momento, tanto emocional como económicamente, por creer en mí, y sacarme al otro lado siempre. Los amo.

A mis hermanos Julio y Giselle, por apoyarme y estar siempre para mí.

A mis familiares, por su apoyo y sus consejos.

A mi familia de la iglesia, especialmente a Soraya y Joel por creer en mí, por apoyarme durante este proceso y llevar cada una de mis metas en sus oraciones.

A los licenciados de la Universidad por compartir sus conocimientos y formarnos profesionalmente, así como a nuestra asesora de contenido MSC. Yaneth Pineda por guiarnos pacientemente en este proceso.

A Steven, por ser parte importante en mi vida, por haberme apoyado y creído en mi T.A.

A mis amigas, por apoyarme y estar ahí en todo el trayecto de la carrera universitaria trabajando juntas. A mis amigas de proceso de grado Helen y María José por acompañarme y ser un excelente equipo.

A mi abuelo Emilio y abuela Santos, que aunque ya no estén con nosotros físicamente, siempre están presentes en mis pensamientos, por haber creído en mí siempre, porque sé que uno de sus sueños era ver este logro hecho realidad ¡YA CASI ABOGADA ABUELOS!

Estephani Gabriela Sánchez Ventura.

INDICE

CAPITULO II

EL DELITO INFORMATICO Y SU REALIDAD PROCESAL EN EL SISTEMA PENAL SALVADOREÑO

CAPITULO III

PRESENTACION, DESCRIPCION E INTERPRETACION DE RESULTADOS

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

ABREVIATURAS

Abreviatura	Concepto
art.	**Articulo**
Cn.	**Constitución de la República de El Salvador.**
CP	**Código Penal vigente.**
CPP	**Código Procesal Penal vigente.**
etc.	**Etcétera.**
TIC´s	**Tecnologías de la Información y Comunicación.**
LECDIC	**Ley Especial de Delitos Informáticos y Conexos.**
FGR	**Fiscalía General de la Republica**
PNC	**Policía Nacional Civil**
CSJ	**Corte Suprema de Justicia**
OEA	**Organización de Estados Americanos**
OCDE	**Organización para la Cooperación y el Desarrollo Económico**
ECOSOC	**Consejo Económico y Social de la Organización de las Naciones Unidas**

INTRODUCCION

La actual investigación denominada “Desafíos del sistema penal salvadoreño en la aplicación de la ley especial contra los delitos informáticos y conexos”, reviste de mucha transcendencia por la criminalidad informática que se está viviendo en la realidad salvadoreña.

En El Salvador, la proliferación de internet ha permitido el desarrollo de nuevos modus operandi para la ejecución de actividades criminales, es decir, el espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables; como difamación, amenaza, estafa, violación a derechos de autor, distribución de pornografía infantil, robo de identidad, la manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. En tal sentido el presente trabajo tiene como objetivo realizar los antecedentes históricos de como surgieron los delitos informáticos, un análisis jurídico -doctrinario sobre la criminalidad informática y la postura de los operadores de justicia.

En la parte I, se desarrolla el proyecto de investigación que comprende el planteamiento del problema, la situación problemática, enunciado del problema, justificación, esto con el objetivo principal de determinar la situación sobre la criminalidad informática y la aplicación de la LECDIC en El Salvador; continuando con un conjunto de objetivos a cumplir durante el desarrollo del trabajo de investigación, y una serie de hipótesis que se fijaron para cumplir con lo pretendido para la investigación.

En la parte II que comprende el capítulo I, se desarrolla la temática de los delitos informáticos desde los antecedentes históricos hasta como llegan

a El Salvador; continuando con el marco doctrinario donde se consignan las diferentes posturas de los autores en cuanto a las características y los bienes protegidos de los delitos regulados en la LECDIC y con el marco legal, que consisten en la protección tanto con leyes internacionales como con leyes nacionales los tipos penales relacionados con la ciberdelincuencia, y la protección de los bienes jurídicos.

En el capítulo II, se desarrolla el cuadro sinopsis de los problemas de investigación, es decir, los temas que tienen vinculación directa con la criminalidad informática en El Salvador; comprendiendo los delitos comunes cometidos mediante sistemas informáticos regulados en la LECDIC, la identificación de casos prácticos posterior a la vigencia de la ley y el impacto que ha tenido esta en la tutela de los bienes jurídicos protegidos, el proceso y las limitaciones del sistema penal para la investigación de los delitos informáticos.

El capítulo III, para la presentación, descripción y análisis de resultados en donde se desenvuelve la respuesta de las personas entrevistadas conocedoras del tema de investigación, mediante el cual cada entrevistado da su postura referente a la aplicación de la LECDIC y los retos y desafíos para una aplicación eficaz; así mismo, se desarrolla el informe final de la investigación, que comprende el logro de objetivos, verificación y demostración de hipótesis.

El capítulo IV, consiste en la presentación de conclusiones y recomendaciones derivadas de los anteriores apartados como una síntesis extraída por el grupo en las cuales se establece la finalidad que tiene la LECDIC en la criminalidad informática salvadoreña y su forma de aplicación.

PARTE I

PROYECTO DE INVESTIGACIÓN

1.0 PLANTEAMIENTO DEL PROBLEMA

1.1 SITUACIÓN PROBLEMÁTICA

Desde el inicio de su invención, se ha podido observar, que la principal finalidad de la creación de la informática, es facilitar algunas de las actividades de los seres humanos a través del uso de los medios tecnológicos. Es evidente el avance que se ha presentado a nivel mundial, respecto a la tecnología, pero el mal uso de todas estas herramientas informáticas, es justamente lo que da paso a múltiples acciones merecedoras de sanciones, ya que, a medida avanza la tecnología con ella los delitos y sus nuevas metodologías y medios para realizarlos, siendo así, que tal circunstancia se convierte en una vía directa para cometer delitos cibernéticos.

A medida que estos delitos se cometían de formas más complejas, surgió la necesidad de su regulación dentro de la legislación salvadoreña ya que, su realización puede llevarse a cabo de forma rápida y sencilla siendo así que en ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

Fue así como surgió la necesidad de la creación de una ley especial que regulara disposiciones referentes a los delitos realizados por medios informáticos, clasificándolos de conformidad al área o al sujeto a que estos delitos se dirigen, obteniendo así la “Ley especial contra delitos informáticos y conexos”, como un medio para la persecución de delitos de esta índole, la cual si bien es cierto, regula delitos realizados por medios informáticos y al encontrarse regulados se entiende que es una acción que la ley prohíbe por lo cual, crea una limitante para un sujeto que quiera realizar cualquiera de los

tipos regulados, pero existe la necesidad que se cuenten con los medios tecnológicos idóneos de investigación para la persecución de estos delitos regulados en la LEDIC.

Rafael Fernández Calvo, define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el Título 1 de la Constitución Española"[1] (Fernandez Calvo, 1996, pág. 1150). Entendiendo al delito como toda conducta típica, antijurídica y culpable constitutiva de infracción penal y en este caso con la variante de utilizar un medio informático, tales como celulares, computadoras entre otras, con la finalidad de vulnerar los derechos de los ciudadanos en general.

Ahora bien, a medida que la tecnología evoluciona, la realización de los delitos se vuelve más sencillo y por otro lado la identificación y persecución de éstos se complica aún más. Estos delitos al ser realizados por medios tecnológicos, se convierten en actos difíciles de demostrar ya que, en muchos casos, es complicado encontrar y conservar las pruebas debido a que no se cuentan con peritos altamente capacitados y al no contar con los medios idóneos de investigación y programas eficaces para la persecución de éstos hace que su persecución se vuelva un obstáculo.

Otra de las problemáticas a la que se enfrenta el sistema penal salvadoreño y específicamente el código Penal es el hecho de que éste no ha avanzado con la velocidad en el que la tecnología lo ha hecho, esto

1 Fernández Calvo, R. (1996). **El Tratamiento del llamado "Delito Informático" en el proyecto de Ley Orgánica del Código Penal**: Reflexiones y propuestas de la GLI. Mérida: UNED. Pág. 1150.

indudablemente constituye un obstáculo, puesto que éste es un tema que ha venido tomando realce en la actualidad.

Se considera que el área informática sigue siendo un ámbito innovador, ya que ésta hizo su aparición en un momento que puede considerarse moderno dentro de la historia salvadoreña, tomando en cuenta que fue a finales del año 1995 cuando se firmó un acuerdo con UUNet un proveedor de internet de Estados Unidos, lo cual hizo posible el envío y recepción de los correos electrónicos dentro del país, dicho envió y recepción no era algo instantáneo puesto que el servidor del El Salvador se conectaba cada media noche con UUNet para así sincronizar los correos electrónicos entre El Salvador y Estados Unidos, lo que significaba que para enviar o recibir un correo podían pasar hasta 24 horas, a pesar de esto, desde ese momento la tecnología ha crecido y evolucionado aceleradamente dentro del país, algo totalmente contrario al ordenamiento jurídico-penal salvadoreño, el cual, fue creado en un periodo en el que no era posible tomar en cuenta el impacto que la nueva tecnología tendría en la sociedad y que ésta podría ser objeto y sujeto para el desarrollo y cometimiento de delitos.

En el ordenamiento jurídico penal y específicamente en referencia al código penal se han visto regulados algunos delitos que contemplan dentro de sí la tecnología, sin embargo esta regulación no pasa de ser vista como u0n agravante, siendo así que la legislación no percibe todavía en la informática o tecnología riesgos en sí mismos como la creadora de situaciones y acciones propias, novedosas constituyentes de delitos y que por su misma característica novedosa son difícilmente protegidas por los tipos tradicionales, por lo tanto se considera que esta regulación no solo debe tomar a la tecnología informática como un medio para la comisión de ciertos

delitos sino además, debe tomarse como un riesgo en sí mismo, es decir, como la creadora de acciones que constituyen delitos.

Ahora bien, a raíz de esto se contempla la necesidad de crear un ordenamiento jurídico que vaya de la mano con las nuevas realidades y así mismo con nuevas herramientas de investigación que permita identificar y comprobar el ilícito considerando que la sociedad es cambiante y con ella se van desarrollando nuevos tipos delictivos, para los cuales es necesario crear un sistema u ordenamiento jurídico suficiente, que sea capaz de regular los nuevos escenarios a los que se enfrentan.

Es así, como se ve la necesidad de crear un marco u ordenamiento adecuado; que se pueda ajustar a estas realidades. Ahora bien, sobre esto también recae la interrogativa de si existe la capacitación o estudio adecuado para las personas encargadas de hacer velar el cumplimiento de dicho ordenamiento, esto con la finalidad de poder resolver este tipo de conductas delictivas, tomando en cuenta que es un ámbito novedoso, lo cual supone que esta persona encargada debe poseer nuevos conocimientos que lo hagan capaz de poder con estos nuevos escenarios, esto considerando que habrá de enfrentarse a nuevos comportamientos por parte de los sujetos que lleven a cabo este tipo de conductas, ahora bien; es por ello que se ve necesario la creación de un mayor manejo informático por parte de especialistas, que se encarguen de capacitar a las personas encargadas de velar por el ordenamiento penal salvadoreño.

1.2 ANTECEDENTE DEL PROBLEMA

Los delitos informáticos, como su nombre lo indica, son aquellos, que se realizan, a través de cualquier medio tecnológico; se define este tipo de delito como: "aquel que se da con la ayuda de la informática o de técnicas

anexas".2 (Callegeri, 1985, pág. 250). Tomando en cuenta para la realización del mismo, toda acción contraria a la ley y en este caso, aquellas ejecutadas a través del uso de medios informáticos, entendiendo a éstos como el ordenador, video interactivo, multimedia y por otro lado el intranet e internet.

En el año de 1969 se estableció ARPANET, la primera red sin nodos centrales, de la que formaban parte cuatro universidades estadounidenses: Universidad de California Los Ángeles (UCLA), Universidad de California Santa Bárbara (UCSB), Universidad de Utah y Stanford Research Institute (SRI) fue creada por el departamento de defensa norteamericano en 1958, para aplicar la tecnología al ámbito militar, esto con el fin de investigar y desarrollar sistemas de comunicaciones eficaces para poder responder en caso de guerra nuclear, esto tuvo gran influencia en el avance de los ordenadores, buscando así la integración de los sistemas que se tendrían que usar en caso de guerra; de forma que estas funcionen correctamente y en tiempo real.

El Internet no se mostraba muy atractivo para el público en general, ya que, al no darse las condiciones el Internet no era considerado un servicio atrayente para la población y esto cambio hasta principios de los años noventa, gracias al británico Tim Berners-Lee quien en los años ochenta, comenzó a diseñar un programa, que permitiera almacenar y recuperar información mediante asociaciones no deterministas.

Partiendo de ese programa, en octubre de 1990 emprendió la elaboración del HTML, que permite combinar texto, imágenes y establecer enlaces a otros documentos. También es creación suya el primer servidor

2 Callegeri, N. (1985). **"Delitos informáticos y legislación" en Revista de la facultad de derecho y ciencias políticas de la Universidad de Pontificia Bolivariana.** Medellín, Colombia. Pág. 250.

World Wide. Al verano siguiente, puso su trabajo en Internet y desde entonces, la Gran Red Mundial (World Wide Web) ha ido extendiéndose de forma exponencial.

Por otro lado, al ver la evolución de los medios informáticos, se determina que el hombre siempre buscó tener dispositivos que le ayudaran a efectuar cálculos precisos y rápidos; de tal forma, que la primera operación de procesamiento de datos fue lograda en 1890 por Hernan Hollerich, quien desarrolló un sistema mecánico para calcular y agrupar datos de censos3 (Herman Holleriths, 1895, pág. 55). El nuevo sistema se basaba en tarjetas perforadas, lo utilizaron en el censo de población en Estados Unidos en donde se logró por primera vez, que los resultados fueran conocidos a los dos años y medio, mientras que el censo anterior se tardó siete años para conocer estos datos.

En 1930, el norteamericano Vannevar Bush diseñó en el MIT (Massachusetts Institute of Technology) el analizador diferencial, marcando el inicio de la era de las computadoras; el "analizador" era una máquina electrónica que media grados de cambio en un modelo. La primera computadora totalmente electrónica fue la ENIAC (Electric Numeric Integrator And Calculator), fue construida en 1943 y 1945 por John Manchi y J. Proper Eckut podía multiplicar 10.000 veces más rápido que la máquina de AIKEN.

Posteriormente, se desarrolló el circuito integrado o "IC" que pronto recibiría el sobrenombre de "chip". Se atribuye el mérito de este invento a Robert Noyce, esta novedad colocó en un finito microchip los circuitos para todas las funciones usuales de un computador. Fueron integrados ahora en

3 Herman Hollerith, B. (1895). **Pionero de la informática por su invención de las maquinas estadísticas de tarjetas o fichas perforadas.** Estados Unidos. Pág. 55.

el chip en una serie de delgadísimas capas. Esto hizo que la computación fuera más rápida y más flexible, al tiempo que los circuitos mejorados permitieron al computador realizar varias tareas al mismo tiempo y reservar memoria con mayor eficacia.

Cuando se habla de informática se define como una de las materias más importantes en la actualidad, ya que por medio de esta vivimos en una sociedad comandada por las nuevas tecnologías, donde la informática juega un papel fundamental en todos los ámbitos, ya que, si bien es cierto, como se mencionaba anteriormente ésta ha venido a facilitar algunas de las actividades realizadas por los seres humanos ayudando así al desarrollo de la sociedad. Así como la tecnología trae consigo una serie de beneficios, el mal uso representa un sinfín de desventajas para la seguridad de la comunidad, siendo esta la que permitió la realización de muchos actos que con posterioridad se consideraría delictivos ya que atentan contra la seguridad cibernética.

Los primeros casos de la delincuencia cibernética se cometieron antes de que internet llegara a existir e implicaba, robo de datos, lo cual es racional, considerando que las computadoras, las redes informáticas e internet se crearon para el almacenamiento y transferencia de información gubernamental y corporativa, información que es de mucha importancia para tales entidades gubernamentales o Estatales.

La informática más que una herramienta, es una ciencia, porque constituye un conjunto de conocimiento de validez universal y fue desarrollada a lo largo de muchos años, avanzando con pasos agigantados, llegando a ser muy importante en la sociedad, cubriendo ámbitos cotidianos de la vida diaria, tales como: correos, chateos, Messenger, etc., hasta cumplir

papeles importantes a nivel laboral, por ejemplo: video conferencias, bases de datos, desarrollos de software y optimización de hardware.

Todo lo antes expuesto, enmarca de forma somera, la razón, por la que, es de vital importancia adquirir nuevos conocimientos y estar a la par con el desarrollo de los mismos, ya que, justamente el uso indebido de las nuevas tecnologías, por no contar con la información adecuada o el respectivo control jurídico, sobre el uso de estas herramientas, ha representado el génesis de los delitos en dicha área.

1.3 ENUNCIADO DEL PROBLEMA

1.3.1 Problema Fundamental

¿Cuáles son las dificultades que presenta el sistema penal salvadoreño al momento de la aplicación de la ley especial contra los delitos informáticos y conexos?

1.3.2 Problemas Específicos

¿Cuál es el proceso correspondiente para una efectiva tramitación de los delitos informáticos?

¿Cuáles son las técnicas de investigación con las que cuenta el sistema penal salvadoreño en la persecución de los delitos informáticos?

¿Qué criterios deben considerar los aplicadores del derecho al momento de dictar una resolución en un proceso referente a los delitos informáticos para el acceso a la justicia?

1.4 JUSTIFICACIÓN

La investigación que se realizará lleva por nombre “Desafíos del Sistema Penal Salvadoreño en la Aplicación de la Ley Especial Contra los Delitos Informáticos y Conexos” el cual cobra importancia dentro de la

realidad salvadoreña por la gran influencia que ha alcanzado la informática en la vida diaria de la humanidad, abriendo de esta manera nuevos medios para la realización de delitos y en este caso, por medios informáticos, ya que, si bien es cierto existen personas que dan una correcta utilidad a estos medios, también existe un porcentaje que crece diariamente de personas muy interesadas en el uso de los sistemas informáticos, que son justamente persona capaces de crear sus propios software con la finalidad de entrar a otros sistemas y cometer delitos o por otro lado un porcentaje de personas que utilizan la tecnología para la obtención de información o material ilícito.

Así mismo, la importancia de este estudio radica en la deficiencia existente en el sistema de investigación y la necesidad de que este sea renovado, puesto que respecto a los delitos informáticos se encuentra cada vez más difícil su persecución, esto gracias a la falta de fronteras en el mundo cibernético, dificultando así la investigación y el procesamiento de estos, si bien es cierto, El Salvador cuenta con el apoyo de la INTERPOL desde el año 2005, la creación del grupo de investigación de delitos informáticos en el año 2011 y el acuerdo para autorizar el inicio de operaciones de la unidad de investigación de delitos informáticos en el año 2015 4 (Rodriguez, 2017), se considera que se cuenta con una gran deficiencia en cuanto a técnicas de investigación para la persecución de los delitos informáticos así como para la obtención de la prueba y el resguardo de esta, siendo esto uno de los principales problemas y un obstáculo para el cumplimiento de la ley.

De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. La posibilidad de su comisión a través de Internet permite que sin

4 Rodríguez, V. M. (marzo de 2017). **Análisis de la Ley de Delitos Informáticos.** Obtenido de Policía Nacional Civil, Subdirecciones de Investigaciones: Sitio Web: www.unodoc.org./Ropan.

mayores complicaciones, el delincuente pueda estar en un determinado país, utilizar servicios de otro, para finalmente atacar a una o más víctimas de un tercer país interviniente.

Dentro de este estudio también se pretende plantear la importancia de garantizar a la víctima que se hará justicia, esto con el fin de que cada persona pueda sentirse segura dentro del medio tecnológico, así mismo tener un sistema penal que cuente con capacidad de dar seguimiento a este tipo de delitos y así descubrir su origen.

Con el paso de los años, la sociedad se ha visto más vulnerable ante el uso de los medios informáticos por lo que, se debe tomar en cuenta que cualquier persona puede ser víctima. Por esta razón, es importante garantizar la seguridad social, tanto colectiva como individual, en el mundo virtual, brindarles información a las personas para que puedan hacer un mejor uso a los medios informáticos y así mismo crear conciencia acerca de los abusos de los que pueden ser víctimas.

Es así, como se considera que la relevancia de realizar esta investigación radica en garantizar la seguridad de la información de las personas, ya que, como se sabe el aspecto de la privacidad, es de gran importancia en la sociedad, en la que día a día se puede observar el fuerte impacto que ha tenido la tecnología, es de esta manera como los seres humanos van confiando cada vez más no solo sus tareas sino también sus datos personales a las redes sin pensar en lo peligroso que esto puede resultar ya que, si bien es cierto el avance de las tecnologías ha venido a facilitar muchas de las tareas, incluso aquellas que pueden resultar un poco complejas; también el desarrollo del internet ha traído consigo una inminente amenaza a la privacidad de sus usuarios invadiendo así la esfera personal y por consiguiente vulnerando los derechos, de esta forma los usuarios pierden

el control sobre sus datos y esto trae consigo una infinidad de posibles actos delictivos que se pueden generar a raíz del robo de datos ya que, no se cuenta con medidas técnicas apropiadas para asegurar la protección de dichos datos, ya sea este contra daños, perdidas, robos o accesos no autorizados, es así como al hacer uso del internet nos encontramos frente a una red que claramente carece de verdaderos niveles de seguridad.

Ahora bien, otro punto por el cual esta investigación es importante, es debido a lo novedosa que es la Ley especial contra los delitos informáticos y conexos para el ordenamiento jurídico salvadoreño, por lo tanto, se debe de tener en cuenta que dentro de este ordenamiento no se cuentan con los conocimientos, ni herramientas adecuadas para su cumplimiento. Sé sabe que cuando se refiere al campo tecnológico se hace referencia a un campo bastante innovador y moderno dentro de la sociedad salvadoreña, por lo tanto, se debe tener en cuenta que el sistema penal salvadoreño debe de contar con las instrumentos necesarias para su investigación y aplicación y así las disposiciones regulada en la LEDIC no se apliquen a medias sino que dicha ley logre el espíritu que busca, que es prevenir los delitos informáticos.

2.0 OBJETIVOS

2.1 Objetivo General

Identificar las dificultades que presenta el sistema penal salvadoreño al momento de la aplicación y tramitación de un proceso de delitos informáticos, y determinar en qué medida esta ley representa una garantía.

2.2 Objetivos Específicos

- Analizar los procedimientos correspondientes a seguir en la tramitación de los delitos informáticos.
- Determinar las técnicas de investigación con las que cuenta el sistema penal salvadoreño en la persecución de los delitos informáticos.
- Examinar cada uno de los criterios a tomar en cuenta por parte de los aplicadores del derecho al encontrarse frente a las deficiencias de investigación en un proceso de delitos informáticos.

3.0 ALCANCES DE LA INVESTIGACIÓN

Con la presente investigación se pretende estudiar un campo tan novedoso como lo es la rama informática, la cual como se sabe ha ido tomando protagonismo dentro del sistema penal salvadoreño en los últimos años por lo que se considera necesario ahondar en el tema realizando un estudio y análisis que nos permita detectar cuáles son las nuevas realidades y retos que dicha rama trae a la sociedad salvadoreña, así mismo cómo se debe responder o reaccionar ante dichas realidades desde la rama jurídica considerando que si bien es cierto, la informática trae consigo numerosos beneficios, está de igual manera implica graves

riesgos frente a los cuales el derecho debe estar preparado para proteger los bienes jurídicos de población.

Así mismo se pretende detallar tanto la importancia que tiene la Ley especial contra delitos informáticos dentro de la legislación Salvadoreña así como los desafíos que ésta enfrenta dentro del sistema penal salvadoreño, considerando que esta ley es bastante novedosa dentro del sistema penal, por lo que se considera necesario estudiar y analizar dicha ley para determinar el grado de protección y garantía que ésta brinda a la población.

3.1 Alcance Doctrinal

Primeramente se entiende la informática como un conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales. Por otro lado Luis Jiménez entiende como delito todo acto típicamente antijurídico, imputable, culpable punible y sujeto, a veces a condiciones objetivas de penalidad.5 (Jimenez de Asua, 2005, pág. 35).

En este sentido los delitos informáticos para Gómez Perals son el conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos6 (Gomez Perals, 1992). Siendo estos delitos que su realización es a través de cualquier medio que

5 Jiménez de Asua, L. (2005). **Teoría Jurídica del Delito**. Madrid, España: Editorial Dyiknso. Pág. 35.

6 Gómez Perals, M. (1992). **Los Delitos Informáticos en el Derecho Español**. España: Unec. Pág. 67.

pertenezca a la informática, por lo que su tratamiento debe de ser especial, adecuada y rápido.

Davara Rodríguez define al Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software7 (Davara Rodriguez, 1990, pág. 45). Siendo esta una acción u omisión que se encuentre tipificada en el sistema penal salvadoreño, se considerada antijurídica, culpable y merecedora de una sanción, y además de estas cualidades su realización sea a través de cualquier medio de la informática.

La doctrina ha denominado a este grupo de comportamientos, de manera genérica: delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática.

La informática se puede decir que está presente casi en todos los ámbitos de nuestra vida moderna, obligando a un porcentaje de la población a rendirse ante lo progresos tecnológicos con el fin de realizar muchas de las tareas que anteriormente se llevaban a cabo de manera manual. Somos una sociedad cambiante y avanzamos muy rápido, anteriormente podíamos estar seguros que nadie más podía acceder a nuestra información sobre nuestra vida privada y asuntos personales, pero esos tiempos han cambiado, puesto que ahora el acceso a la información privada de una persona, puede verse expuesta gracias a la creación de estos sistemas capaces si bien es cierto, de almacenar cantidad de información pero también de transmitirla.

7 Davara Rodríguez, M. A. (1990). **Análisis de la Ley de Fraude Informático**, Revista de Derecho. El Salvador: UNAM. Pág. 45.

Algunos autores se han referido al proceso de desarrollo de la influencia la tecnología informática como: la segunda revolución industrial, que sus efectos pueden ser aún más transformadores que los de la industrial del siglo XIX.8 (Sieber, 1992, pág. 65).

En este sentido, el uso indebido de los medios informáticos ha generado la manipulación de información con la finalidad de realizar daños a segundas personas por el mal uso de la información a la cual pueden tener acceso.

Todos estos avances tecnológicos, y todo a lo que nos han expuesto, genero la iniciativa de la creación de una ley que sirviera de medio de protección para intervenir a la hora de la comisión de conductas delictivas realizadas por medios informáticos, obteniendo como resultado en nuestro sistema penal salvadoreño mediante Decreto Legislativo No. 260 de fecha 26 de febrero de 2016, la Ley Especial contra Delitos Informáticos y Conexos, como un medio para garantizar la seguridad de nuestra información en el uso de medios electrónicos, por lo que es responsabilidad del Estado facilitar las herramientas que sean necesarias a las instituciones responsables para una mejor aplicación de dicha ley.

Actualmente los delitos informáticos en El Salvador se encuentran regulados en una ley especial, con la finalidad de prevenir y sancionar conductas delictivas que tengan como finalidad el uso o el acceso indebido a la información de segundas personas. Tomando en cuenta que Los casos de delito informático más reportados por agencias de policía en el continente americano incluyen la producción, distribución y posesión de pornografía infantil. Sin embargo la creación de la ley antes citada podría no ser suficiente

8 Sieber, U. (1992). **Documentación Para Aproximación al Delito Informático**. Barcelona, España: Editorial. PPU. Pág. 65.

garantía, si no se cuentan los las herramientas necesarias, así como con los conocimiento precisos para la correcta aplicación de esta ley.

En el desarrollo del marco teórico del presente trabajo, se abordaran todos estos aspectos de manera detenida con la finalidad que profundizar en cada uno de estos puntos, tanto como su origen, historia hasta los desafíos que podría presentar nuestro sistema penal salvadoreño en la aplicación de la Ley especial contra los delitos informáticos y conexos.

3.2 Alcance Jurídico

El tema “desafíos del sistema penal salvadoreño en la aplicación de la ley especial contra los delitos informáticos y conexos” es de mucha relevancia debido a que, todos estos medios informáticos no siempre son utilizados como una herramienta de ayuda o apoyo para la realización de algunas de nuestras actividades diarias, si no que por otro lado, son utilizadas como un medio eficaz para la obtención de información con una finalidades delictiva.

En relación con lo anterior, la legislación penal de El Salvador vigente desde el año 1998, marginalmente hacía referencia al cometimiento del delito mediante el uso de las tecnologías de la información y la comunicación, utilizando términos como “a través de medios electrónicos”, como en los artículos 172 y 346 del CP, “informática” o “virtual”, como en el 173 del mismo cuerpo legal, por lo que tal regulación lo hacía de forma asistemática y esporádica. Pero en atención a la falta de regulación en el código penal en cuanto a los delitos informáticos, lo cual representaba inseguridad hacia los sistemas informáticos y los datos personales, Actualmente contamos con la Ley Especial contra Delitos Informáticos y Conexos aprobada el 26 de febrero de 2016.

En el presente trabajo tomara como base de la investigación, algunos criterios a considerar dentro de la aplicación de la Ley especial contra los delitos informáticos, haciendo un estudio de una manera genérica de los que esta trata.

3.3 Alcance teórico

En el desarrollo del presente trabajo se hará una breve mención de algunos autores que en sus obras tratan el tema de delitos informáticos, es así como entre ellos se toma como una delas principales referencias doctrinarias al autor Julio Téllez Valdez, quien en su obra titulada “Derechos Informáticos” define al delito informático como “Aquellas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin” o "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin".9 (Tellez Valdez, 1991)

Así mismo se encuentra al tratadista Carlos Sarzana, quien se ha pronunciado acerca de los delitos informáticos y establece que son “cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo”.10 (Sarzana, 1979, pág. 33).

En dicha definición, se observa que se menciona a los delitos informáticos tanto como un medio, es decir como un material, así como también como un fin es decir un objetivo, en cuanto a la primera categoría se puede establecer que se hace referencia a conductas delictivas que se valen de las computadoras como símbolo para llevar a cabo el ilícito, mientras que en la segunda categoría se hace referencia a las conductas ilícitas que se

9 Téllez Valdez, J. (1991). **Derecho Informático**. México: 1a Edición. Pág. 345.

10 Sarzana, C. (1979). **Criminalista y Tecnología, los Crímenes por Computadora**. Roma, Italia: COMMIN. Pág. 33.

dirigen directamente en contra de la computadora o programa como una entidad física.

Ahora bien, Nidia Callegari define al delito informático como “Aquel que se da con la ayuda de la informática o de técnicas anexas” en cuanto a este concepto se puede observar como la autora únicamente percibe a la informática solamente como un medio para el cometimiento de los delitos.11 (Callegeri, 1985, pág. 97)

Miguel Ángel Davara Rodríguez, define a los delitos informáticos como “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnere los derechos del titular de un elemento informático”.12 (Davara Rodriguez, 1990, pág. 85).

María Cinta Castillo, entiende al delito informático como “toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas”13 (Castillo Jimenez, 1989, pág. 456).

Marcelo Huerta y Claudio Líbano, definen los delitos informáticos como “todas aquellas acciones u omisiones, típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la victima a través de atentados a la sana técnica informática, lo cual generalmente, producirá de

11 Callegeri, N. (1985). "**Delitos informáticos y legislación" en Revista de la facultad de derecho y ciencias políticas de la Universidad de Pontificia Bolivariana**. Medellín, Colombia. Pág. 97.

12 Davara Rodríguez, M. A. (1990). **Análisis de la Ley de Fraude Informático**, Revista de Derecho. El Salvador: UNAM. Pág. 85.

13 Castillo Jiménez, M. C. (1989). **El Delito Informático**. Zaragoza: Congreso Sobre Derecho Informático. Pág. 456.

manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro”14 (Huerta Miranda, 1998, pág. 45).

Ahora bien, al interpretar todas las definiciones dadas anteriormente, recaemos en que el termino delito informático puede utilizarse en forma plural siendo así que el delito informático no solamente se concentra en una forma específica de delito sino que éste término supone una pluralidad y multiplicidad de modalidades y conductas delictivas vinculadas con las computadoras.

3.4 Alcance Temporal

Este alcance es de mucha importancia dentro de la investigación, puesto que con este se pretende establecer el tiempo y duración de la misma, esto para poder realizar las investigaciones necesarias referente al tema y cumplir con todos aquellos requisitos y factores que se exigen dentro de la investigación, es así como el presente trabajo de investigación se enmarcara dentro del periodo correspondiente a nuestros años de estudio, es decir, del año 2014 al presente año, tiempo que se considera razonablemente justo para poder llevar a cabo un estudio amplio del problema objeto de estudio, el cual hace referencia a los desafíos del sistema penal salvadoreño en la aplicación de la ley especial contra los delitos informáticos y conexos.

3.5 Alcance espacial

El presente tema de investigación ha representado un impacto no solo nacional sino mundial, pero tendrá un área geografía que abarca la zona ori ental de El Salvador puesto que el tema de investigación pretende identificar los desafíos en el sistema penal salvadoreño como tal, al momento de la ap

14 Huerta Miranda, M. C. (1998). **Los Delitos Informáticos**. España: Cono Sur. Pág. 45.

licación de la ley especial contra los delitos informáticos y conexos. Haciend o consultas en diferentes entes gubernamentales para un mejor desarrollo d el tema objeto de estudio, entre ellos: la Fiscalía General de la Republica, la Policía Nacional Civil. Así mismo se pretende llevar a cabo consultas con def ensores privados que hayan trabajado con la ley especial contra los delitos i nformáticos y conexos, con la finalidad de escuchar las opiniones respecto a los desafíos con los que podrían encontrarse al momento de aplicar estar le y en la práctica.

4.0 SISTEMA DE HIPÓTESIS

4.1 Hipótesis General

Frente al inminente avance de las tecnologías y el uso indebido de estas, el sistema penal salvadoreño se vio en la necesidad de la creación de la ley especial contra los delitos informáticos y conexos, como garante del sistema informático y datos personales; sin embargo en la practica el sistema penal podría presentar diferentes desafíos para la correcta aplicación de la ley.

4.2 Hipótesis Específicas

Hipótesis específica 1.

El proceso común es totalmente eficaz dentro del sistema penal salvadoreño frente a las exigencias de la ley especial contra los delitos informáticos y conexos.

Hipótesis especifica 2.

La falta de herramientas específicas para la persecución de los delitos informáticos vuelve ineficaz la LEDIC.

Hipótesis especifica 3.

Si bien es cierto, los delitos informáticos se encuentran regulados en una ley especial, como garantía del sistema informático, sin embargo, al no contar la FGR y LA PNC con las herramientas y conocimientos en el ejercicio práctico, esta ley perdería su objetivo como garante de la seguridad de la informática.

CAPITULO I

ANTECEDENTES HISTÓRICOS – BASE DOCTRINAL – BASE CONCEPTUAL – BASE LEGAL.

1.1 ANTECEDENTES HISTÓRICOS DEL DELITO INFORMATICO

En este apartado nos interesa determinar el nacimiento de la delincuencia informática; para ello es necesario realizar una aproximación a la historia del internet para luego abordar la historia del delito informático propiamente, en razón de un marco de referencia exacto y en virtud, de que, es a través de éste fenómeno que se prolifera el Delito Informático.

1.1.1 ORIGEN DEL INTERNET

Aníbal Pardini hace referencia a que el inicio del INTERNET, se remonta a 1969, cuando la Agencia de Proyectos de Investigación Avanzada en Estados Unidos, conocida por sus siglas, "ARPA" (Avancé Research Projects Agency), desarrolló ARPANET, una especie de red que unía redes de cómputo del ejército y de laboratorios universitarios que hacían investigaciones sobre la defensa.15 (Pardini, 2002, pág. 33).

“Esta red, permitió primero a los investigadores de Estados Unidos acceder y usar directamente súper computadoras localizadas en algunas universidades y laboratorios clave”16 (Pardini, 2002, pág. 34); después, compartir archivos y enviar correspondencia electrónica. A finales de 1970 se crearon redes cooperativas descentralizadas, como UUCP, una red de comunicación mundial basada en UNIX y USENET (red de usuarios), la cual daba servicio a la comunidad universitaria y más adelante a algunas organizaciones comerciales.

En 1980, las redes más coordinadas, como CSNET (Acrónimo en inglés de Red de Ciencias de Cómputo), y “BITNET (red de gran extensión que conecta instituciones de educación superior en E.E.U.U., usada principalmente para divulgar avances en investigaciones y noticias del

15 Pardini, A. A. (2002). **Derecho de Internet**. Buenos Aires, Argentina: La Rocca. Pág. 33.

16 Ibídem Pág. 34.

ámbito académico”.17 (Climent, Barrera, 2001) Su nombre proviene del inglés Because It´s Time Network, es decir, ‘porque ya era hora’), empezaron a proporcionar redes de alcance nacional, a las comunidades académicas y de investigación, las cuales hicieron conexiones especiales que permitieron intercambiar información entre las diferentes comunidades. En 1986, se creó la Red de la Fundación Nacional de Ciencias (NSFNET, acrónimo en inglés), la cual unió en cinco macrocentros de computo a investigadores de diferentes Estados de Norte América, de este modo, esta red se expandió con gran rapidez, conectando redes académicas a más centro de investigación, remplazando así a ARPANET en el trabajo de redes de investigación. ARPANET se da de baja en marzo de 1990 y CSNET deja de existir en 1991, cediendo su lugar a INTERNET.

La red se diseñó para una serie descentralizada y autónoma de uniones de redes de computo, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa comercial alguna y con la habilidad automática de reentrar datos si una o más uniones individuales se dañan o están por alguna razón inaccesibles.

“Cabe señalar que entre otros objetivos, el sistema redundante de la unión de computadoras se diseñó para permitir la continuación de investigaciones vitales y comunicación cuando algunas partes de ésta red se dañaran por cualquier causa”.18 (Lopez Ortega, 2001)

Gracias al diseño de Internet, y a los protocolos de comunicación en los que se basan un mensaje enviado por éste medio puede viajar por

17 Climent, Barrera, J. (2001). **Conferencia la Justicia Penal en Internet. Territorialidad y competencias penales, Consejo General del Poder Judicial (pág. 75).** Estados Unidos: Biblioteca Judicial Fernando Coto

18 López Ortega, J. J. (2001). **Conferencia Libertad de expresión y r5esponsabilidad por contenidos en internet. Consejo General del Poder Judicial (pág. 75).** Estados Unidos: Biblioteca Judicial Fernando Coto.

cualquiera de diversas rutas, hasta llegar a su destino, y en caso de no encontrarlo, será reentrado a su punto de origen en segundos.

Una de las razones del éxito de Internet, es su interoperabilidad, es decir, su capacidad para hacer que diversos sistemas trabajen conjuntamente para comunicarse, siempre y cuando los equipos se adhieran a determinados estándares o protocolos, que no son sino reglas aceptadas para transmitir y recibir información.

El espíritu de la información que se maneja en Internet es que sea pública, libre y accesible a quien tenga la oportunidad de entrar a la red, lo cual marca un principio universalmente aceptado por los usuarios y que ha dado lugar a una normativa sin fronteras y de lo cual podemos deducir, en términos jurídicos, cuál sería la ratio iuris o razón de ser de esta especial normatividad.

Se intenta que Internet, sea, un medio interactivo viable para la libre expresión, la educación y el comercio. No existe institución académica, comercial, social o gubernamental que pueda administrarla. Son cientos de miles de operadores y redes de cómputo, que de manera independiente, deciden usar los protocolos de transferencia y recepción de datos para intercambiar comunicaciones, información. No existe un lugar que concentre o centralice la información de Internet, Sería técnicamente imposible.

“Los individuos tienen una amplia gama de formas de introducirse al Internet, a través de los proveedores de acceso a Internet, conocidos en el medio de las telecomunicaciones como Internet Service Provider”.19 (Devoto, 2001, pág. 100) En términos de acceso físico, se puede usar una computadora personal, conectada directamente (por cable coaxial o de

19 Devoto, M. (2001). **Comercio Electrónico y firma digital: las regulaciones del ciberespacio y las estrategias globales.** Buenos Aires, Argentina: La Ley S.A., primera edición. Pág. 100.

fibra óptica) a una red (un proveedor de servicios de Internet, por ejemplo), que éste a su vez, conectada a Internet; o puede hacerse una computadora personal con un módem conectado a una línea telefónica a fin de enlazarse a través de ésta a una computadora más grande o a una red, que esté directa o indirectamente conectada a Internet.

Ambas formas de conexión son accesibles a las personas en una amplia variedad de Instituciones académicas, gubernamentales o comerciales. Lo cierto es que hoy en día el acceso a la red de Internet es cada vez más sencillo en Universidades, bibliotecas y ciber cafeterías, lo cual está estrechamente relacionado con el número de proveedores de servicios de Internet.

Los servicios más importantes que brinda el INTERNET, en general son los siguientes: a) CORREO ELECTRÓNICO, siendo el servicio de mayor uso, de mayor tráfico y, por lo tanto, de mayor importancia para el surgimiento, en la actualidad, de diversas relaciones contractuales. Permite escribir y enviar mensajes a una persona o grupo de personas conectadas a la red; b) TRANSFERENCIA DE ARCHIVOS, el cual permite transferir archivos, los cuales pueden ser de texto, gráficas, hojas de cálculo, programas, sonido y vídeo. c) ACCESO REMOTO A RECURSOS DE COMPUTO POR INTERCONEXIÓN, (telnet), es una herramienta interactiva que permite introducirse, desde una computadora en casa o en la oficina, a sistemas, programas y aplicaciones disponibles en otra computadora, generalmente ubicada a gran distancia y con gran capacidad; d) WORD WIDE WEB, el servicio más nuevo y popular de Internet, caracterizado por la interconexión de sistemas a través del hipertexto, por medio del cual pueden transmitirse textos, gráficas, animaciones, imágenes y sonido. Se le considera un elemento importante de mercadotecnia. e) GRUPOS DE DISCUSIÓN (Usenet), existen hoy día alrededor de quince mil grupos enfocados a diversos temas, en la actualidad se llega alrededor de cien mil mensajes por día; f)

COMUNICACIÓN EN TIEMPO REAL, es la posibilidad de establecer diálogos inmediatos en tiempo real, a través de Internet, permitiendo a dos o más personas "dialogar" simultáneamente por escrito, sin importar la distancia geográfica. “Esta forma de comunicación es análoga a la línea de teléfono, sólo que emplea el teclado o monitor en lugar del auricular”.20 (Rodriguez, Martinez, 2001, pág. 75)

1.1.2 ANTECEDENTES DEL INTERNET EN EL SALVADOR

En septiembre de 1994 se gestionó, ante el IANA (Internet Assigned Numbers Authority, es decir, Autoridad de Número Asignados de Internet) y el InterNIC (Internet Network Information Center, es decir, Centro de Información de la Red Internet), respectivamente, un conjunto de direcciones IP, equivalentes a una clase B, y la administración del dominio de Nivel Superior correspondiente a El Salvador, SV. “Ese mismo mes y año, el grupo SVNet fue constituido por la Universidad Centroamericana UCA, el CONACYT (Consejo Nacional de Ciencia y Tecnología), la UES (Universidad de El Salvador), la Universidad Don Bosco, ANTEL (Agencia Nacional de Telecomunicaciones) y FUSADES (Fundación Salvadoreña del Desarrollo), con el fin de administrar ambos recursos”. 21 (Superintendencia General de Electricidad, 2013)

En octubre de ese año se estableció un acuerdo con UUNet, en Virginia, EEUU, para manejar el tráfico de correo desde y hacia El Salvador, bajo el dominio SV. En diciembre se instaló y configuró exitosamente uno nodo UUCP (Unix to Unix Copy Program) de correo electrónico en el CONACYT con este propósito, y los primeros mensajes con direcciones terminadas en SV comenzaron a circular en Internet.

---

20 Rodríguez, Martínez, L. J. (2001). **Conferencian Los virus informáticos y el delito de daños. Consejo General del Poder Judicial (pág. 75).** Estados Unidos: Biblioteca Judicial Fernando Coto.

21 UNODOC. **Superintendencia General de Electricidad, T. (23 de marzo de 2013)**. Obtenido de Boletín Estadístico de Telecomunicaciones: https://www.siget.gob.sv/temas/telecomunicaciones/estadistica/boletin-estadistico/

Como anécdota curiosa, se puede referir que los primeros mensajes venían escritos en ruso, pues algunas personas pensaban que SV eran las siglas de la extinta Unión Soviética.

Anteriormente y junto a esta iniciativa, era posible intercambiar correos a través de Internet por vías tales como la ofrecida por ANTEL, usando el protocolo X.25, o a través de los servicios de otros nodos UUCP, como el llamado Huracán. La provisión del servicio de correo electrónico a los salvadoreños que así lo desearan, con direcciones SV, inició en marzo de 1995. Esto era realizado por medio de una llamada telefónica a medianoche a UUNet, en la que se intercambiaban los mensajes de y hacia nuestras direcciones SV y el resto del mundo.22 (Devoto, 2001, pág. 101)

En paralelo, y desde la constitución de SVNet, se había venido trabajando en la formulación de un proyecto a presentar a la OEA (Organización de Estados Americanos), en el marco del proyecto RedHUCyT (Red Hemisférica Universitaria de Ciencia y Tecnología). Finalmente, después de varias revisiones y ajustes, el proyecto salvadoreño fue presentado por SVNet a la OEA en septiembre de 1995.

Se llevaron a cabo varios eventos relacionados, entre ellos dos WorldNets, en la Embajada de los Estados Unidos (Julio y Octubre de 1995) con panelistas nacionales e internacionales vía satélite, varios cursos y seminarios organizados por diversas instituciones, un panel técnico sobre "Criterios para la gestión y desarrollo de la red Internet en El Salvador", y otros. La capacitación técnica a los miembros de SVNet fue realizada por los mismos salvadoreños, en noviembre.

22 Devoto, M. (2001). **Comercio Electrónico y firma digital: las regulaciones del ciberespacio y las estrategias globales.** Buenos Aires, Argentina: La Ley S.A., primera edición. Pág. 101.

Después del trabajo de conexión y pruebas realizadas en diciembre de 1995, ese mismo mes se firmó un convenio de mutua colaboración entre ANTEL y los demás miembros de SVNet, que posibilitó la instalación de líneas dedicadas a estas instituciones. Enero de 1996 vio un punto de presencia a Internet estable desde El Salvador, así como la recepción de los equipos que la OEA había financiado para iniciar la conectividad a Internet de nuestro país.

En febrero de 1996 ANTEL completó la instalación de los primeros enlaces dedicados a Internet en territorio salvadoreño, siendo éstos el de la Universidad Centroamericana José Simeón Cañas y el de la Universidad Don Bosco. El siguiente mes vieron surgieron los sitios web de estas dos universidades, así como los de SVNet y la página principal de (www.sv), convirtiéndose así en los primeros sitios web de El Salvador que residían en un servidor ubicado físicamente en El Salvador. Desde entonces, el crecimiento de Internet en El Salvador ha sido, como en todo el mundo, gratamente acelerado.

En cuanto a la capacidad instalada, todos los proveedores de conectividad y servicios Internet han incrementado y modernizado continuamente dicha capacidad, motivados por la demanda, que también ha ido en crecimiento. Se estima que este crecimiento es del orden de un 20% anual. Por la misma razón, y para mantenerse activos en el mercado, todas las empresas desarrollan planes de expansión con una programación en el tiempo que consideran, acertadamente, una de sus piezas de información más celosamente guardadas.

“En este campo, no es raro que las empresas vayan siendo absorbidas, vendidas o fusionadas por otras, en algunos casos internacionales, en otros por empresas que originalmente se hallan en otra

línea de negocio pero desean explotar el servicio de conectividad en El Salvador".23 (Rivas, 2012, pág. 45)

Algunos de los equipos utilizados en la provisión del servicio por las empresas dedicadas a ello comprenden:

- ✓ Enrutadores Cisco 2500, 3600, 3640, 7206 para conexiones proveedores y backbones.
- ✓ Equipos de enrutamiento Cisco 1720 para clientes dedicados.
- ✓ Equipos de acceso Cisco AS5300 con capacidad de 4 E1s cada uno.
- ✓ Servidores Compaq para Mail Server, Web Server, Hosting, Monitoreo.
- ✓ Equipos con plataforma Solaris, Linux y AIX.

Algunos de los servicios ofrecidos por las empresas consideradas Proveedores de Servicios Internet (ISPs) en el país son:

- ✓ Accesos conmutados
- ✓ Accesos dedicados
- ✓ Alojamiento de sitio Web (Web Hosting)
- ✓ Web TV
- ✓ Video conferencia a través de IP
- ✓ Diseño de páginas Web
- ✓ Servicios de soporte a servidores de Internet

23 Rivas, J. (2012). **Historia de la Computación.** El Salvador: Comunicaciones Informáticas. Pág. 45.

- ✓ Diseño, Instalación y configuración de redes LAN y WAN
- ✓ Asesoría en adquisición de sistemas de comunicación de datos
- ✓ Capacitación a empresas
- ✓ Desarrollo de aplicaciones orientadas o basadas en tecnología Internet, tales como Intranet y sistemas bancarios
- ✓ Telefonía Computarizada
- ✓ Servicios de acceso satelital

A diferencia de la telefonía, la provisión de servicios relacionados con Internet, como tales, no requieren de una autorización por parte de la Superintendencia General de Electricidad y Telecomunicaciones (SIGET). Esto ha propiciado que aun empresas de relativo pequeño tamaño, hayan visualizado éste como un negocio productivo, y se hallen decididos a perseverar y obtener una cuota importante de un mercado en continuo crecimiento, en El Salvador como en el resto del mundo.

En lo que tiene El Salvador de estar permanentemente conectado a Internet, como se dijo anteriormente, desde febrero de 1996, y considerando la fecha presente, han llegado a existir más de veinte empresas proveedoras de servicios de conectividad a Internet. Algunas de estas empresas han sido absorbidas por otras, nacionales o internacionales, otras más han surgido en distintos años, y muchas de las empresas tienen entre sus actividades la provisión de otros servicios, desde el alojamiento de páginas Web hasta la telefonía tradicional (fija, móvil, internacional, o todas).

1.1.3 SURGIMIENTO DE LOS DELITOS INFORMATICOS A NIVEL INTERNACIONAL

En el año de 1977 la primera propuesta de legislar el delito informático fue la introducida por el Senador Ribicoff en el Congreso

Federal de Estados Unidos. Años después, en 1983, la OECD (Acrónimo en inglés de Organization for Economic Co-operation and Development, es decir, Organización de Cooperación y Desarrollo Económico u OCDE) en París, designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los Códigos Penales, como resultado de las propuestas de este comité, la OCDE recomendó a sus países miembros la modificación de su legislación penal, a los efectos de que la misma pueda aplicarse a ciertas categorías de delitos informáticos. La propuesta incluía una lista de actas que podían constituir un común denominador.

En el año de 1983 la Organización de Cooperación y Desarrollo Económico (OCDE u OECD, en su acrónimo en inglés) con el fin de proteger el uso indebido de programas de computación, inició un estudio sobre la posibilidad de armonizar las leyes penales en el plano internacional. Como consecuencia de dicho estudio en 1986 publicó un informe, llamado "Delitos de Informática: análisis de la normativa jurídica" con las recomendaciones sobre cuáles serían los usos indebidos que los distintos países podrían prohibir y sancionar a través de sus leyes penales.

En el año de 1989 el Consejo de Europa convocó a otro comité de expertos, que en la Recomendación número 89 adoptada el 13 de septiembre de 1989, presenta una lista mínima de los delitos sobre los que debía necesariamente legislarse en cada país miembro, y una lista opcional.

En el año de 1990 el tema fue también discutido en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado en Montreal en 1990, en el octavo Congreso Criminal de las Naciones Unidas celebrado en La Habana el mismo año y en la Conferencia de Wurzburgo, Alemania, en 1992.

En el año de 1995 el Consejo de Europa adopta en Septiembre de 1995, otra recomendación concerniente a los problemas de derecho procesal conectados con la Información Tecnológica.

En el año de 1996 el Comité Europeo para los Problemas Criminales (CDPC, acrónimo en francés de Comité Européen pour les Problèmes Criminels) decidió en noviembre de 1996 establecer un nuevo comité de expertos para que se abordaran el tema de los delitos informáticos. Con relación a la decisión del CDPC, el Comité de Ministros estableció el nuevo comité denominado: "Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras (PC-CY)" por decisión nº CM/Del/Dec 97-583, tomada en la 583ª reunión de los Representantes de los Ministros (celebrada el 4 de febrero de 1997).

En los años de 1997- 2000 el Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras (PC-CY), inició su labor en abril de 1997 y efectuó negociaciones con respecto al borrador de un convenio internacional en materia de delitos informáticos. Entre abril de 1997 y diciembre de 2000, el Comité PC-CY celebró 10 reuniones plenarias y 15 reuniones de su Grupo de Redacción. Se levantó el secreto a una primer versión del borrador del Convenio y se la publicó en abril de 2000, seguida por borradores que fueron publicados después de cada reunión plenaria, con el fin de posibilitar que los Estados negociadores la realización de consultas con todas las partes interesadas. Este proceso de consulta resultó muy útil.

El borrador del Convenio revisado y finalizado y su Memorando Explicativo fue sometido para su aprobación al CDPC en su 50ª sesión plenaria en junio de 2001, después de lo cual el texto del borrador del Convenio fue sometido a consideración del Comité de Ministros para su aprobación y quedó abierto para su firma.

En el año de 1990’s – Actualidad prácticamente desde la década de los años noventa distintos países del mundo comenzaron a regular en sus respectivos ordenamientos jurídicos lo concerniente a los delitos informáticos, con el fin de crear o establecer seguridad y prevenir esta nueva forma de criminalidad.

1.1.4 SURGIMIENTO Y EVOLUCION DEL ORDENAMIENTO JURIDICO PENAL EN MATERIA DEL DELITO INFORMATICO

Desde que el Internet llego a El Salvador el uso de las nuevas tecnologías digitales y de la telefonía inalámbrica se empezó a generalizar, estas tecnologías brindaban la libertad para moverse y permanecer comunicados y conectados con miles de servicios construidos sobre redes de redes, daban la posibilidad de participar; de enseñar y aprender, de jugar y trabajar juntos, y de intervenir en el proceso político. A medida que las personas dependían cada vez más de estas tecnologías, era necesario utilizar medios jurídicos y prácticos eficaces para prevenir los riesgos asociados. Las tecnologías de la sociedad de la información a pesar que producían cambios de desarrollo también podían utilizarse para perpetrar y facilitar diversas actividades delictivas en manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público.

Contra el desarrollo de las nuevas tecnologías para el año de los noventa se aprobó el Código Procesal Penal por Decreto Legislativo No. 1030, 26 de Abril del 1997, fue publicado en el Diario Oficial No. 85, Tomo No. 335 del 13 de Mayo de 1997, y entró en vigencia el día 20 de Enero de 1998, dicho Código regula algunas conductas en ciertos tipos penales en los que la informática aparece como un medio para la comisión de tipos autónomos y distintos a los delitos informáticos.

En el año 2000 en El Salvador había aproximadamente 40,000 usuarios de internet por lo era una “amenaza” en expansión; no obstante, el acceso a internet puede ser considerado un indicador de desarrollo, así como una ventana de oportunidad, esto no es siempre el caso. Del número de usuarios en aumento, ya sea a través de banda ancha o dispositivos móviles, deriva un aumento del número casos de delito informático/cibercrimen, así como de ciberdelincuentes. Una encuesta aplicada sobre agencias de aplicación de la ley en 69 países en el contexto de un estudio de UNODC, mostro que “para el periodo 2007 2011, el número de casos reportados de delito informático/cibercrimen se había incrementado significativamente.”

En el año 201224 (UNODOC, Direccion General de Estadisticas y Censos, Ministerio de Economia: Estimaciones y Proyecciones de Poblacion Nacional 2005-2050, 2016, pág. 27) El Salvador contaba con una población a 6,090,646 de habitantes, un porcentaje de 1,491,480 usuarios de internet y con un 1,491,480 de usuarios de Facebook, lo que significaba que cada día el internet llegaba a más personas y existía un creciente acceso a la tecnología y a una globalización social de la información, por lo que la proliferación de internet permitió el desarrollo de nuevos modus operandi para la ejecución de actividades criminales como difamación, amenaza, estafa, violación a derechos de autor, distribución de pornografía infantil, robo de identidad, entre otras.

En el año 2016 25 (UNODOC, La Droga y el Delito, 2016) debido al creciente número de caso de delitos informáticos y en razón de la casi carente regulación o lo asistemático de la misma, en el Código Penal y

24 UNODOC. (2016). **Dirección General de Estadísticas y Censos, Ministerio de Economía: Estimaciones y Proyecciones de Población Nacional 2005-2050.** San Salvador: Cybercrime. pág. 27.

25 UNODOC. (2016). **La Droga y el Delito**. El Salvador: Oficina de Naciones Unidas, Documentos Internos.

demás leyes especiales en cuanto a los delitos informáticos que atentan contra la seguridad de los sistemas informáticos, la integridad de los datos informáticos y que afectan otros bienes jurídicos cometidos por medio del uso de las TIC's, así como contra el bien jurídico indemnidad sexual de niños, niñas y adolescentes, además como personas con discapacidad mental, mediante Decreto Legislativo No. 260 de fecha 26 de febrero de 2016, publicado en el Diario Oficial No. 40, Tomo No. 410, de fecha 26 de febrero de 2016, se aprobó la Ley Especial contra Delitos Informáticos y Conexos (en adelante LECDIC), la cual entró en vigencia 8 días después de su publicación en el Diario Oficial (art. 36), es decir el 6 de marzo de 2016 (art. 140 de la Constitución), hace necesaria la actualización de los diversos operadores de la justicia penal en su contenido.

1.1.4.1 Ciberataque detonante para creación de LEDIC

La presidenta de la Asociación E-Safe Teens y abogada experta en ciberdelitos, Miriam Guardiola, comentó que la Ley Especial contra Delitos Informáticos de El Salvador, que fue creada el año pasado, "es una ley muy completa", pero "existe mucho desconocimiento por parte de la población". Los ataques cibernéticos en contra de LA PRENSA GRÁFICA) fue el punto de inflexión para que se regulara este tipo de delitos informáticos. Quizá fue el detonante" para la creación de la Ley Especial contra Delitos Informáticos en El Salvador, en donde la fiscalía acuso a Mayra Lisseth Morán, Óscar Domínguez y Sofía Medina, gerente de Comunicaciones de la Alcaldía de San Salvador, de organizarse para planear y ejecutar la clonación del sitio web de este rotativo para publicar notas falsas. Uno de esos ataques ocurrió el 7 de julio de 2015, cuando difundieron una entrevista falsa del presidente de LA PRENSA GRÁFICA, José Roberto Dutriz.

La experta en ciberdelitos participó en una conferencia sobre el tema en un hotel capitalino, la cual fue organizada por la revista Derecho y Negocios. En las ponencias se expusieron casos prácticos y famosos de

algunos delitos cibernéticos internacionales y nacionales, entre los cuales se mencionó el ciberataque del virus Wanna Cry, el cual afectó a cerca de 150 países durante este año. También se discutió el caso LPG, del cual se tocaron los puntos del “límite entre libertad de expresión y vulnerabilidad del derecho a la intimidad y propiedad de la imagen, también de la usurpación y suplantación de identidad”, explicó Guardiola.

Al congreso asistieron despachos de abogados, peritos informáticos, docentes, diputados y empresarios.

En cuanto al evento, el presidente de la revista Derechos y Negocios, Manuel Carranza, dijo que ha sido de mucha ayuda para analizar a profundidad la Ley Especial Contra Delitos Informáticos. “Nosotros lo que hemos estado analizando son las consecuencias que tienen muchos actos que se están dando en El Salvador que la gente no saben que son condenables, no saben que hay una ley o un artículo en específico que dice que si tú comentes eso, serás sancionado”, explicó el presidente de la revista Derechos y Negocios.

Al igual que Guardiola, Carranza coincidió en que en el país el tema de los ciberdelitos es poco conocido; sin embargo, existe mucho interés por parte de la población para querer disolver las dudas sobre los mismos. “Es un tema que se desconoce mucho, no solo a nivel general, sino que los mismos abogados desconocen de la materia. Muchos de ellos no sabían que existe una ley ni las consecuencias de la misma”, expresó Carranza.

De igual forma, los expertos expusieron el tema de los ‘memes’, el cual tiene mucha relevancia actualmente por el alto consumo de redes sociales en el país. “Se habló de los casos de los ‘memes’ y en qué momento el ‘meme’ se entiende como sátira y en qué momento pasa las barreras y empieza a dañar el honor, la imagen de las personas, y eso se puede convertir en un juicio civil”, indicó Carranza, quien considera que

esta será una de las herramientas más utilizada durante las campañas electorales.

Actualmente, la Ley en El Salvador condena la violación de la seguridad del sistema, estafa informática, espionaje informático, daño a la integridad y disponibilidad de los datos, hurto de identidad, utilización de datos personales, interferencia de datos, entre otros crímenes relacionados.

1.2 BASE DOCTRINAL

1.2.1 GENERALIDADES DE LA DELINCUENCIA INFORMATICA

Hoy en día es difícil establecer solamente un tipo de delincuente, debido que a medida que se han desarrollado aspectos culturales, educativos, científicos, tecnológicos, de igual forma ha ido desarrollando la delincuencia en muchos ámbitos como los tecnológicos, y propiamente en materia informática, y tal es así que muchos de los estudiosos del amplio mundo del derecho han realizado fenomenales esfuerzos mentales para el establecimiento de posturas en un inmenso mundo de la información a través de los medios informáticos.

El aspecto más importante de la informática radica en que la información ha pasado a convertirse en un valor económico de primera magnitud. “Desde siempre el hombre ha buscado guardar información relevante para usarla después”. 26 (Magliona, Markovicth & & Lopez Medel, 1999, pág. 51) Como señala Camacho Losa, “En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de

26 Magliona, Markovicth, C. P., & & López Medel. (1999). **Delincuencia y Fraude Informático.** Chile: Editorial Jurídica. Pág. 51.

la historia.”27 (Camacho, Losa, 1987, pág. 124) Entonces el autor se pregunta ¿y por qué la informática habría de ser diferente?

Existe un consenso general entre los diversos estudiosos de la materia, en considerar que el nacimiento de esta clase de criminalidad se encuentra íntimamente asociada al desarrollo tecnológico informático. Las computadoras han sido utilizadas para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato. Los primeros casos fueron reportados en 1958. Para el profesor Manfred Mohrenschlagereste fenómeno ha obligado al surgimiento de medidas legislativo penales en los Estados Industriales donde hay conciencia de que en los últimos años, ha estado presente el fenómeno delictivo.28 (Mohrenschlager, 1992, pág. 99).

1.2.1.1 Delincuencia informática y Abuso Informático

Gómez Perals la define como el conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.29(Gómez Perals, 1994, pág. 32).

Ruiz Vadillo recoge la definición que adopta el mercado de la OCDE en la Recomendación número R 81-12 del Consejo de Europa indicando que abuso informático “es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos”.

---

27 Camacho, Losa, L. (1987). **El Delito Informático**. Madrid España: Civetas. Pág. 124.

28 Mohrenschlager, M. (1992). **El Nuevo Derecho Penal Informático**. Alemania: Cono Sur. Pág. 99.

29 GÓMEZ PERALS, M. (1994) “**Los Delitos Informáticos en el Derecho Español**”. España: Editorial Aranzadi Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25. Pág. 32.

La misma definición aporta Correa incidiendo en la Recomendación 89-9, del Comité de Ministros del Consejo de Europa considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el computador.

1.2.1.2 Criminalidad informática

Baón Ramírez define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

Tiedemann[30] (Tiedemann, 1985, pág. 34) considera que con la expresión “criminalidad mediante computadoras”, se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.

Como el mismo autor señala, el concepto abarca el problema de la amenaza a la esfera privada del ciudadano, y por otra parte, se refiere además a los daños patrimoniales producidos por el abuso de datos procesados automáticamente.

Para Carlos Sarzana, en su obra Criminalità e tecnología, los crímenes por computadora comprenden “cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo”.

30 Tiedemann, K. (1985). **El Poder Informático.** Barcelona, España: Civetas. Pág. 34.

1.2.2 DEFINICION Y CONCEPTO DE DELITO INFORMATICO

Nidia Callegari define al delito informático como “aquel que se da con la ayuda de la informática o de técnicas anexas. Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también que lo informático puede ser el objeto de la infracción”.31 (Callegeri, 1985, pág. 23)

Davara Rodríguez define al Delito informático como, “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software”.32 (Davara Rodriguez, 1990, pág. 17)

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” y por las segundas “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”.33 (Tellez, Valdes, 1996, pág. 56)

Parker define a los delitos informáticos como “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio”34 (Romeo Casanoba, 2003, pág. 33)

---

31 Callegeri, N. (1985). **"Delitos Informáticos y Legislación" en revista de la Facultad de Derecho y Ciencias Políticas de la Universidad de Pontificia Bolivariana**. Medellín Colombia. Pág. 23.

32 Davara Rodríguez, M. A. (1990). **Análisis de la Ley de Fraude Informático, Revista de Derecho.** San Salvador: UNAM. Pág. 17.

33 Téllez, Valdés, J. (1996). **"Los Delitos Informáticos".** México: 1º Edición.

34 PARKER, D.B, Citado por Romeo Casabona Carlos M. (2003) **Poder Informático y Seguridad Jurídica.** España. Civetas. Pág. 33.

María Cinta Castillo y Miguel Ramallo entienden que "delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas"35. (Jimenez Castillo, 1989, pág. 31)

1.2.3 ELEMENTOS DE LOS DELITOS INFORMATICOS

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. “Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo”.36 (Huerta Miranda, 19990, pág. 129).

El delito de daños informáticos se configura como un delito común, por lo que el sujeto puede ser cualquier persona física o jurídica, siempre que no sean los titulares de los datos, programas informáticos, documentos electrónicos o sistemas informáticos.

1.2.3.1 Sujeto Activo

El sujeto activo del delito, lo constituye la persona física que con su conducta produce el resultado lesivo para el pasivo, lesionando o poniendo en peligro el bien jurídicamente tutelado.

---

35 Jiménez Castillo, M. (1989). **El Delito Informático, Congreso Sobre Derecho Informático.** Zaragoza, España: Civetas. Pág. 31.

36 Huerta Miranda, M. & Libano Manzur, C (19990). **Los Delitos Informáticos.** España: Cono Sur. Pag.129.

Para Chavarría en los delitos informáticos y electrónicos las personas que lo cometen los son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, es aquel individuo que tiene dominio del hecho, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.37 (Chavarria, 2016).

1.2.3.2 El sujeto activo desde el punto de vista Criminológico

Según el criminológico norteamericano Edwin Sutherland, señala que el Sujeto Activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional, pero con conocimiento en informáticos. Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como Delitos de cuello blanco.38 (Tellez, Valdes, 1996, pág. 34), así mismo, podemos decir, que el sujeto activo de los delitos informáticos no se determina de acuerdo al bien jurídico protegido que se lesa, como sucede en los delitos convencionales, sino de acuerdo al sujeto activo que los comete.

El delincuente tecnológico comúnmente asume una actitud de reto con los sistemas a que se enfrenta, de modo tal que considera

37 Chavarría, A. R. (12 de 06 de 2016). **Delitos Informáticos. Obtenido de Legislación y manejo de la Información:** www.ictparliamet.org/sites/default/files/delitosinformaaticos.

38 Téllez, Valdés, J. (1996). "**Los Delitos Informáticos**". México: 1º Edición. Pág. 164

suficientemente justificado el lucro que obtiene, como recompensa a su pericia e inteligencia.

En la ponencia titulada "Incidencia de las Nuevas Tecnologías de la Información en el Derecho Penal", celebrado hace algún tiempo en Caracas, la Profesora Española Mariluz Gutiérrez Francés refería en lo siguiente:

El computador es un factor criminógeno de primera magnitud que aporta a la conducta criminal, unas veces, un nuevo objeto (la información misma, potenciada y revaluada por los nuevos sistemas de procesamiento de datos y los programas), y otras, un nuevo instrumento: ofreciendo un inmenso abanico de técnicas y estrategias que pueden ponerse al servicio del delito, enriqueciendo el repertorio criminal. Esta acertada distinción permite precisar cuando la tecnología es medio y cuando objeto del delito.

Cuando la información se convierte en objeto de apropiación y en blanco lucrativo del delincuente, se ven afectados valiosos bienes jurídicos como la intimidad, el orden socioeconómico, la fe pública y la seguridad del estado, entre otros.

1.2.3.3 El sujeto activo según sus Características

Las personas que pueden cometer Delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Estas características nos remiten a:

a) Operadores, que se pueden poner en relación con el Sistema para modificar, agregar, eliminar, sustituir información y/o programas, copiar archivos para venderlos a competidores.

b) Programadores, que pueden violar o inutilizar controles protectores del programa y/o sistema; dar información a terceros ajenos a la empresa, atacar el sistema operativo, sabotear programas, modificar archivos, acceder a información confidencial.

c) Analistas de sistemas, que pueden solucionarse con usuarios, programadores y/u operadores para revelarles la operación de un sistema completo.

d) Analistas de comunicaciones, que enseñan a otras personas la forma de violar la seguridad del sistema de comunicaciones de una empresa, con fines de fraude.

e) Supervisores, que pueden en razón de su oficio manipular los archivos de datos y los ingresos y salidas del sistema.

f) Personal técnico y de servicio, que por su libertad de acceso al centro de cómputo puede dañar el sistema operativo.

g) Ejecutivos de la computadora, que pueden actuar en situación de colusión con otras personas.

h) Auditores, que pueden actuar como los anteriores.

i) Bibliotecarios de preparación, que pueden vender la documentación.

j) Bibliotecarios de operaciones, que pueden destruir información mediante errores o pueden venderla a competidores.

k) Personal de limpieza, mantenimiento y custodia, que pueden vender el contenido de los costos de papeles, fotocopiar documentos, sabotear el sistema.

l) Usuarios, que pueden modificar, omitir o agregar información con fines fraudulentos.

Para Del pino “Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes”.39 (De Pino, 2016).

1.2.3.4 El Sujeto Pasivo

Para Chavarría “En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros”.40 (Chavarria, 2016, pág. 33).

“El sujeto pasivo, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos”.41 (Chavarria, 2016, pág. 33).

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables" y si a

39 Del Pino, S. A. (18 de 06 de 2016). **Delitos Informáticos. Obtenido de Generalidades:** http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.

40 Chavarría, A. R. (12 de 06 de 2016). **Delitos Informáticos. Obtenido de Legislación y manejo de la Información:** www.ictparliamet.org/sites/default/files/delitosinformaaticos.

41 Ibídem

esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas.

Por lo anterior, se reconoce que, para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento".

1.2.3.5 Bien Jurídico Protegido

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir, ya que constituye la razón de ser del delito, y no suele estar expresamente señalado en los tipos penales.42 (De Pino, 2016, pág. 20)

1.2.3.6 Bienes jurídicos Protegidos en los Delitos Informáticos

Dentro de los delitos informáticos, los bienes jurídicos protegidos la interpretación se hace desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos.

Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para

42 Del Pino, S. A. (18 de 06 de 2016). **Delitos Informáticos. Obtenido de Generalidades:** http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.

facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

De otro lado otra vertiente doctrinaria supone que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible. Esto por cuanto la información no puede a criterio de Pablo Palazzi ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual está constitucionalmente protegida.

En fin la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de “dañosidad” o “lesividad”. Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada, que inspira tanto a la criminalización como a descriminalización de conductas. Su origen directo es la teoría del contrato social, y su máxima expresión se encuentra en la obra de Beccaria “Los Delitos y las Penas” (1738 -1794).

Se define como un bien vital, “bona vitae”, estado social valioso, perteneciente a la comunidad o al individuo, que por su significación, es garantizada, a través del poder punitivo del Estado, a todos en igual forma.

En conclusión se puede decir que el bien jurídico protegido en general es la Información, pero está considerada en diferentes formas, ya sea como un valor económico, o como valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan

o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tales como:

a) Las personas.

b) El honor de las personas.

c) La intimidad de las personas.

d) La propiedad (de hardware o software).

e) Los Documentos, archivos, registros, bases de datos, y toda información concerniente al que hacer propio de la Entidad.

f) La fe pública.

Por lo que el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere, para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir “que se caracterizan porque simultáneamente protege varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo”.43 (Reyes Echandia, 1981, pág. 32).

En fin, podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y por último, por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales.

El nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes(intimidad,

43 Reyes Echandia, A. (1981). **La Tipicidad**. Colombia: Universidad de Externado. pág. 32.

seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa.

Un ejemplo que puede aclarar esta situación, es el de un hacker que ingresa a un sistema informático con el fin de vulnerar la seguridad éste y averiguar la información que más pueda sobre una determinada persona, esto en primer lugar se puede decir que el bien jurídico lesionado o atacado es el derecho a la intimidad que posee esa persona al ver que su información personal es vista por un tercero extraño que sin autorización ha vulnerado el sistema informático donde dicha información está contenida. Pero detrás de ese bien jurídico encontramos otro un bien colectivo que conlleva a un ataque a la confianza en el funcionamiento de los sistemas informáticos. Es decir, de intereses socialmente valiosos que se ven afectados por estas nuevas figuras, y que no solo importan la afección de bienes jurídicos clásicos.

1.2.4 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

En lo que respecta a las características se podrá observar el modo de operar de estos ilícitos:

a) Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas;

b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando;

c) Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico;

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios de más de cinco cifras a aquellos que los realizan;

e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse;

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho;

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar;

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico;

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención;

j) Ofrecen facilidades para su comisión a los mentores de edad;

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación;

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Luego de todo lo mencionado se puede indicar de forma concreto de las características enunciadas que es importante señalar que se debe de actuar de la manera más eficaz para evitar este tipo de delitos y que no se sigan cometiendo con tanta impunidad, debido a que si no se conoce de la materia, difícilmente se podrán crear y aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular.

1.2.5 EL DELITO INFORMATICO Y SU IMPACTO A NIVEL SOCIAL

1.2.5.1 La sociedad y el delito informático

El Internet tiene un impacto profundo en el mundo laboral, el ocio y el conocimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea.

Comparado a las enciclopedias y a las bibliotecas tradicionales, la web ha permitido una descentralización repentina y extrema de la información y de los datos.

Con el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar computadoras conectadas, en regiones remotas. Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa de información y de una interactividad que sería inaccesible de otra manera.

No ponemos en duda que el progreso de la tecnología, ha traído aparejado un sinfín de beneficios, avances económicos, de comunicación, culturales y ha facilitado el acceso y la distribución de la información. Pero al mismo tiempo puso en peligro los derechos a la intimidad, y a la libertad de los individuos, como así también la seguridad de los sistemas informáticos, entre algunas de sus desventajas. Es aquí cuando la sociedad moderna, tiene que poner un freno a las consecuencias de estos avances y controlarlos.

La posibilidad de gran almacenamiento que poseen estos sistemas, como así también su fácil distribución, ha llevado a que mucha información privada, haya sido violada, o utilizada con un fin distinto al que propuso su autor. Muchos han utilizado estos ordenadores para ocultarse y así cometer amenazas o calumnias e injurias, con total impunidad.

En estos años, las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online superan los 250 millones, comparado con 26 millones en 1995. Técnicamente es imposible lograr un sistema informático ciento por ciento seguros, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos. Para ello, es necesario la Implementación de barreras de seguridad antivirus, anti-espías, encriptación de la información y uso de contraseñas.

1.2.5.2 Impacto a nivel social

"La proliferación de los delitos informáticos ha hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general".44 (Landaverde Contreras, 2000, pág. 45) Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general.

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más, están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global.

Las empresas que poseen activos informáticos importantes, son más celosas y exigentes en la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos. Aquellas personas que no poseen los

44 Landaverde Contreras, M. &. (2000). **Delitos Informáticos.** San Salvador: Universidad de El Salvador. Pág. 45.

conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. En vista de lo anterior aquel porcentaje que no conoce nada de informática, por lo general personas de escasos recursos económicos, pueden ser engañadas si en un momento dado, poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etc.

La falta en la sociedad de cultura informática puede ser un gran impedimento para la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

1.2.6 EL DELITO INFORMATICO Y LA TEORIA DEL DELITO

En el presente punto se hará un breve análisis a la luz de la Teoría del Delito, sobre los caracteres esenciales que se han ido desarrollando en los puntos anteriores, como configuradores específicos del delito informático.

En esta óptica, el derecho penal, se ha visto transformado en sus formas y ámbitos de intervención, aparecen en conductas que emplean medios no convencionales para la comisión de hechos ilícitos creándose problemas en el momento de su sanción. El impacto de la explosión tecnológica es un problema que la política criminal conoce sobradamente. La técnica siempre es un arma y cada avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen. En este sentido para desarrollar la teoría del delito es necesario conceptualizar al delito como… “una acción típicamente antijurídica y culpable, de acuerdo a ella los elementos constitutivos del delito son acción tipicidad, antijuricidad y culpabilidad.”45 (Harb, 2003, pág. 12).

45 Harb, M. B. (2003). **Derecho Penal.** La Paz, Bolivia: Editorial Juventud. Pág. 12.

“La Teoría del Delito es una teoría de la aplicación de la ley penal, y como tal pretende establecer un orden para el planteamiento y la resolución de los problemas que implica la aplicación de la ley penal, en materia penal esto encuadra a lo que se conoce como tipo que define y establece los elementos del delito.”46 (Harb, 2003, pág. 14) La misma cumple una doble función mediadora, por un lado entre la ley y la solución del caso concreto y por otro lado, una mediación entre la ley y los hechos que son objeto del juicio. Se denomina así al estudio del conjunto de elementos del delito considerados como partes autónomas, mediante las cuales es posible aprender el concepto unitario, aunque complejo, de la infracción punible, por tanto ningún acto humano puede ser reprochado como delito, sí una ley no lo prohíbe previamente, para ello, es necesario comprobar que alguien se comportó de la manera prevista en la ley, que dicho comportamiento no se encontraba autorizado en las circunstancias en que tuvo lugar, y por último, que el autor de dicho comportamiento tenía las condiciones personales requeridas para poder responsabilizarlo por la conducta realizada.

Ahora analizaremos estos elementos desde la óptica particular de la temática, objeto de la presente investigación.

1.2.6.1 Principio de Legalidad

El Principio de Legalidad, exige como condición esencial, la existencia de un régimen jurídico que formule la descripción del hecho o conducta criminal y de la pena a imponerse, previamente al hecho que califica a ella como criminal, para imputar a una persona como autora del delito. La concreción legislativa de nuevos supuestos de incriminación que supongan nuevos delitos, es un paso importante que se llevó a cabo en la legislación salvadoreña con la creación de la LECDIC.

46 Ibídem Pág. 14.

A nivel mundial existen varios pronunciamientos y reformas legislativas tendientes a la protección de bienes jurídicos o intereses como ser el software, la información, la intimidad, etc., debemos remarcar que dicha nueva normativa, brinda una solución parcial a la problemática que nos ocupa.

1.2.6.2 Principio de Reserva Penal

El Principio de Reserva Penal, se encuentra en la garantía de la legalidad. Es decir, que el ámbito de lo punible debe estar determinado exhaustivamente por la ley, y que todo lo que queda al margen de ese ámbito está reservado como esfera de impunidad.

“El Principio de Reserva presupone como condiciones de su existencia, las siguientes: La determinación legal de los hechos punibles, la determinación legal de las penas correspondientes, la prohibición de la analogía y la irretroactividad de la ley penal.”47 (Nuñez, 1987, pág. 83) La problemática de los delitos informáticos, en relación al principio de reserva resta aclarar que la garantía individual está antes del derecho penal: se refiere a la facultad de actuar del hombre dentro de lo permitido48 (Creus, 2004, pág. 55), sin que su conducta pueda acarrearle sanción alguna. O sea que es una garantía del individuo, no directamente ante los organismos de “persecución”, sino ante el mismo órgano de legislación penal: este no puede asignar una pena a una conducta que esté permitida por el ordenamiento jurídico, antes tiene que prohibirla.

La doble garantía del principio de reserva (una limita la libertad de punir, y la otra la de prohibir), tienen una especial importancia en el análisis de las nuevas figuras delictivas en el ámbito de la informática. Debemos considerar – especialmente en nuestra legislación actual -, la necesidad

47 Núñez, R. (1987). "**Manual de Derecho Penal".** Córdoba: Editorial Heliasta. Pág. 83

48 Creus, C. (2004). "**Derecho Penal, Parte General".** Buenos Aires, Argentina: Editorial Buenos Aires. pág. 55.

de distinguir entre software y hardware; siendo el primero el elemento lógico del sistema informático (programas), y el segundo el elemento material (maquinaria, aparatos, etcétera).

1.2.7 DERECHO COMPARADO SOBRE EL REGULAMIENTO DEL DELITO INFORMATICO

1.2.7.1 Costa Rica

La legislación costarricense entorno al desarrollo de cuerpos jurídicos que regulan al delito informático se puede catalogar como innovadora. Los primeros tipos penales informáticos fueron regulados a partir del año 2001, cuando se crearon e incluyeron en el Código Penal los delitos de violación de comunicaciones electrónicas, fraude electrónico y alteración de datos y sabotaje informático, los cuales son modificados con la nueva ley, Ley 9048 —Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal‖ aprobada el 6 de noviembre del año 2012.

Con esta ley se brinda especial protección a la niñez del —Uso doloso e irresponsable de la tecnología de la información‖ ya que los tipos penales existentes eran abiertos e imprecisos. Así mismo con esta legislación, se crea un instrumento jurídico para abordar nuevas situaciones que surgen a partir de la ciberdelincuencia.

1.2.7.2 Nicaragua

Nicaragua en materia de regulación de Delitos informáticos no ha desarrollado una estrategia o política de seguridad cibernética nacional concreta, que brinde seguridad de forma eficaz a sus gobernados que hacen uso de esta nueva herramienta tecnológica, ya que los instrumentos jurídicos que regulan algunas de estas conductas se encuentran dispersos en distintas leyes entre las cuales podemos mencionar: Constitución Política de Nicaragua, Ley 641 Código Penal de la Republica de Nicaragua

y Ley 831 Ley que reforma la Ley número 49, Ley de amparo que contiene el recurso de Habeas Data. Lo que impiden que las víctimas de delitos informáticos sepan que instrumento jurídico debe invocarse cuando están frente a este tipo de hechos (Delitos Informáticos).

Si bien es cierto que Nicaragua no cuenta con un instrumento jurídico especializado que de tratamiento a la delincuencia informática, esto no quiere decir que algunos tipos penales o bien algunas conductas criminales no se prevengan o sancionen. Puesto que, como dijimos anteriormente si se previenen en diversos cuerpos normativos.

1.2.7.3 México

Mediante una reforma publicada el 6 de junio de 2007 se modifica el Código Penal Federal de México, con el objeto de penalizar las conductas relacionadas con la corrupción de menores e incapaces, pornografía infantil y prostitución sexual de menores, delitos en materia de derechos de autor, revelación de secretos y acceso ilícito a sistemas y equipos de informática.

El delito informático con mayor pena de prisión en México es "Transmitir, elaborar, reproducir, vender, arrendar, exponer o publicitar material que contenga grabaciones de actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de 18 años" (Gobierno de México, 2007).

1.2.7.4 Argentina

Mediante la Ley 26388, del 4 de junio de 2008, se modifica la Ley 11179, Código Penal de la Nación Argentina, con el objeto de incorporar y sustituir del código referido varios artículos regulatorios de los delitos informáticos.

El Senado y Cámara de Diputados argentinos, reunidos en congreso, sancionaron la sustitución del epígrafe del capítulo iii del título v

del libro ii de su Código Penal, definiéndolo como "Violación de secretos y de la privacidad", el cual castiga y tipifica las conductas punibles como aparece a continuación:

El delito informático con mayor pena de prisión es "Defraudar con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de trucos o engaños, mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de sistemas informáticos" (Senado y Cámara de Diputados de la Nación de Argentina, 2008).

En marzo de 2010, Argentina fue invitada a adherirse al Convenio sobre la Ciberdelincuencia por parte del Consejo de Ministros del Consejo de Europa.

1.2.7.5 Colombia

Mediante la Ley 1273, del 5 de enero de 2009, se modifica el Código Penal Colombiano con el objeto de crear un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos", además de preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

El Congreso de Colombia decreta la adición al Código Penal del título vii bis, "De la protección de la información y de los datos", el cual se compone únicamente de dos capítulos, a saber:

El delito informático con mayor pena de prisión en Colombia es el hurto por medios informáticos y semejantes, el cual consiste en superar medidas de seguridad informáticas para apoderarse de una cosa mueble ajena, con el fin de obtener provecho para sí o para otro, mediante la manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante o mediante la suplantación de un

usuario ante sistemas de autenticación y de autorización establecidos (Congreso de la República de Colombia, 2009).

El 11 de septiembre de 2013, Colombia fue invitada a adherirse al Convenio sobre la Ciberdelincuencia, por parte del Consejo de Ministros del Consejo de Europa.

1.2.7.6 República Dominicana

El Congreso Nacional de la República Dominicana dispone la Ley 53 del 2007, sobre "crímenes y delitos de alta tecnología", cuyo objeto es la protección integral de los sistemas de tecnologías de la información y comunicación, su contenido, la prevención y sanción de las conductas punibles cometidas contra estos o las cometidas mediante el uso de tecnología en perjuicio de las personas.

Los delitos informáticos con mayor pena de prisión en esta nación son los siguientes:

• "El sabotaje, espionaje o suministro de informaciones, a través de un sistema informático, electrónico, telemático o de telecomunicaciones, atentando contra los intereses fundamentales y seguridad de la Nación" (Congreso Nacional de la República Dominicana, 2007).

• "Ejercer actos de terrorismo, con el uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones" (Congreso Nacional de la República Dominicana, 2007).

La República Dominicana es el primer país latinoamericano en ratificar el Convenio sobre la Ciberdelincuencia, debido a que a principios de 2013 ratificó su adhesión como Estado no miembro del Consejo de Europa, convenio que entró en vigor en junio del mismo año, siendo a partir de ese momento un modelo para Sur y Centroamérica.

1.2.7.7 España

Mediante la Ley Orgánica 10 del 23 de noviembre de 1995, las Cortes Generales y el rey de España aprobaron y sancionaron el Código Penal vigente, el cual incluye la tipificación de la delincuencia informática.

El delito informático con mayor pena de prisión en este país es la "Alteración, copia, reproducción o falsificación de tarjetas de crédito o débito o cheques de viaje; así como la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de la conducta referida" (las Cortes Generales y el rey de España, 1995).

España es un modelo de referencia en este campo, debido a su condición de Estado miembro del Concejo Europeo, firmó el convenio del cibercrimen el 23 de noviembre del 2001, realizando su última ratificación el 3 de junio de 2010 y entrada en vigor el 1.º de octubre del mismo año.

1.2.7.8 El Salvador

El Salvador en materia de delitos informáticos está avanzando en cuanto a su cuerpo legislativo reglamentaria, puesto que el pasado 26 de febrero del 2016 dio un paso importante en esta materia aprobando la Ley 260 ¨Ley Especial Contra los Delitos Informáticos y conexos¨.

La ley se inspira en el reconocimiento de la persona humana como el origen y el fin de la actividad del Estado, quien como garante de justicia, seguridad jurídica y bien común, debe brindar especial protección a sus ciudadanos, debido a la diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación cuyo daño representa severas repercusiones en materia de política, economía y el desarrollo tecnológico.

Dichos comportamientos criminales se encontraban anteriormente regulados de forma dispersa en diferentes instrumentos jurídicos tales

como: Decreto Nº 1030 Código Penal, El Salvador, Decreto Nº 534, Ley de Acceso a la Información Pública y Decreto Nº 133, Ley de Firma Electrónica, entre otras. Las cuales no eran suficientes para brindar la protección necesaria y eficaz, generándose cierta impunidad para quienes cometen estos tipos de delitos; en consecuencia, resultó necesario la adopción de mecanismos suficientes para facilitar su detección, investigación y sanción de estos nuevos tipos de delitos.

1.3 BASE CONCEPTUAL

Delito Informático: se considerará la comisión de este delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información;

Bien Jurídico Protegido: es la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros;

Datos Informáticos: es cualquier representación de hechos, información o conceptos en un formato digital o análogos, que puedan ser almacenados, procesados o transmitidos en un sistema informático, cualquiera que sea su ubicación, así como las características y especificaciones que permiten describir, identificar, descubrir, valorar y administrar los datos;

Medio de Almacenamiento de Datos Informáticos: es cualquier dispositivo a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo;

Sistema Informático: es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información;

Comunicación Electrónica: es toda transmisión de datos informáticos, cuyo contenido puede consistir en audio, texto, imágenes, videos, caracteres alfanuméricos, signos, gráficos de diversa índole o cualquier otra forma de expresión equivalente, entre un remitente y un destinatario a través de un sistema informático y las demás relacionadas con las Tecnologías de la Información y la Comunicación;

Dispositivo: es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la Tecnología de la Información y la Comunicación;

Interceptar: es la acción de apropiarse, interrumpir, escuchar o grabar datos informáticos contenidos o transmitidos en cualquier medio informático antes de llegar a su destino;

Programa Informático: es la rutina o secuencia de instrucciones en un lenguaje informático determinado que se ejecuta en un sistema informático, pudiendo ser éste un ordenador, servidor o cualquier dispositivo, con el propósito que realice el procesamiento y comunicación de los datos informáticos;

Proveedor de Servicios: es la persona natural o jurídica que ofrece uno o más servicios de información o comunicación por medio de sistemas informáticos, procesamiento o almacenamiento de datos;

Tráfico de Datos Informáticos: son aquellos que se transmiten por cualquier medio tecnológico, pudiendo mostrar el origen, destino, ruta, hora, fecha, tamaño, duración de la comunicación, entre otros;

Tecnologías de la Información y la Comunicación: es el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros;

Datos Personales: es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar;

Datos Personales Sensibles: son los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral, familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la propia imagen, a la intimidad personal y familiar;

Material Pornográfico de Niñas, Niños y Adolescentes: es toda representación auditiva o visual, ya sea en imagen o en vídeo, adoptando un comportamiento sexualmente explícito, real o simulado de una persona que aparente ser niña, niño o adolescente adoptando tal comportamiento. También se considerará material pornográfico, las imágenes realistas que representen a una niña, niño o adolescente adoptando un comportamiento sexualmente explícito o las imágenes reales o simuladas de las partes genitales o desnudos de una niña, niño o adolescente con fines sexuales;

Tarjeta Inteligente: es el dispositivo que permite mediante la ejecución de un programa la obtención de bienes, servicios, propiedades o información;

Redes Sociales: es la estructura o comunidad virtual que hace uso de medios tecnológicos y de la comunicación para acceder, establecer y

mantener algún tipo de vínculo o relación, mediante el intercambio de información.

Sistema penal: es el control social penitenciario institucionalizado. Además, es el conjunto de vínculos y procesos resultados del ejercicio de la facultad penal del Estado. Lo que permite llevar las relaciones del control penal, que no se encuentren dentro de los límites jurídicos, denominados fuera del límite.

Política criminal: Es ésta el conjunto de respuestas que un Estado estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción.

Delito: delito es un comportamiento que, ya sea por propia voluntad o por imprudencia, resulta contrario a lo establecido por la ley. El delito, por lo tanto, implica una violación de las normas vigentes, lo que hace que merezca un castigo o pena.

Pena: una pena es la condena, la sanción o la punición que un juez o un tribunal impone, según lo estipulado por la legislación, a la persona que ha cometido un delito o una infracción.

Criminalidad: Es un conjunto de acciones consideradas ilegales y que son perseguidas por la policía y castigadas por la justicia. Y dentro del marco de la delincuencia, se encuentra el crimen, una acción considerada como especialmente grave.

Computadora: es un dispositivo informático que es capaz de recibir, almacenar y procesar información de una forma útil. Una computadora está programada para realizar operaciones lógicas o aritméticas de forma automática.

Hardware: es la parte física de un ordenador o sistema informático. Está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y luz, placas, memorias, discos duros, dispositivos periféricos y cualquier otro material en estado físico que sea necesario para hacer que el equipo funcione.

Software: es un término informático que hace referencia a un programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático. Comúnmente se utiliza este término para referirse de una forma muy genérica a los programas de un dispositivo informático, sin embargo, el software abarca todo aquello que es intangible en un sistema computacional.

El sujeto activo del delito: es quien participó, de algún modo, en la comisión del hecho delictivo, es decir, es la persona física que como autor, partícipe o encubridor, intervino en la comisión del delito.

Sujeto Pasivo del Delito: es quien sufre directamente la acción, es sobre quien recaen todos los actos materiales utilizados en la realización del ilícito, es el titular del derecho dañado o puesto en peligro. Pueden ser sujetos pasivos del delito: el hombre individual, las personas colectivas, el Estado y la colectividad social.

1.4 BASE LEGAL

La creación de nuevas tecnologías permite crear un mundo más novedoso y formas nuevas de relación dentro de éste, la informática comienza a crear espacios de interacción entre las personas que ya no pueden ser protegidos por los tipos penales tradicionales, por eso la necesidad de tipificar algunas acciones propias de la informática en la

legislación salvadoreña, siendo una facultad que otorga la Constitución de la Republica para resguardar la seguridad de las personas.

1.4.1 LEYES INTERNACIOANLES

1.4.1.1 Convención Sobre Delitos Informáticos (BUDAPEST)

Artículo 7 - Falsificación informática

Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte puede exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 - Fraude informático

Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a) cualquier introducción, alteración, borrado o supresión de datos informáticos;

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Artículo 9.- Delitos relacionados con la pornografía infantil

1 Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) la difusión o transmisión de pornografía infantil por medio de un Sistema informático,

d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2 A los efectos del anterior apartado 1, por pornografía infantil se entender· todo material pornográfico que contenga la representación visual de:

a) un menor comportándose de una forma sexualmente explícita;

b) una persona que parezca un menor comportándose de una forma sexualmente explícita;

c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3 A los efectos del anterior apartado 2, por menor se entender· toda persona menor de 18 años. No obstante, cualquier Parte podrá· establecer un límite de edad inferior, que ser· como mínimo de 16 años.

1.4.2 LEYES NACIONALES

1.4.2.1 Constitución de la Republica de El Salvador

Art 1.- El Salvador reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecución de la justicia, de la seguridad jurídica y del bien común.

La seguridad jurídica es “la certeza de la vigencia y la aplicación de la ley, tanto en los gobernantes como en los gobernados, sin discriminación ni parcialidad”. Si el Estado está organizado para la consecución de la seguridad jurídica, y ésta es la certeza de la vigencia y la aplicación de la ley que tiene la población, podemos afirmar que no puede haber tal si en el diario vivir de las personas se dan cierto tipo de relaciones que estén fuera de cualquier control jurídico, tal como es el caso de los delitos informáticos en el país.

Según la Constitución, la persona humana debe tener seguridad jurídica, y para lograr la consecución de ésta, el Estado debe tomar las acciones necesarias y precisas. En este caso, debe tomar una acción desde el marco jurídico-penal, para cubrir aquellos espacios generados por el desarrollo de la informática que han quedado fuera de toda regulación y que por lo tanto generan inseguridad jurídica para toda una población que cada vez depende más de dicha tecnología.

1.4.2.2 Ley Especial Contra los Delitos Informáticos y Conexos

La ley se inspira en el reconocimiento de la persona humana como el origen y el fin de la actividad del Estado, quien como garante de justicia, seguridad jurídica y bien común, debe brindar especial protección a sus ciudadanos, debido a la diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación cuyo daño representa severas repercusiones en materia de política, economía y el desarrollo tecnológico.

Acceso Indebido a Sistemas Informáticos

Art. 4.- El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, será sancionado con prisión de uno a cuatro años.

Acceso Indebido a los Programas o Datos Informáticos

Art. 5.- El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de la Información o la Comunicación, accediera parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será sancionado con prisión de dos a cuatro años.

Interferencia del Sistema Informático

Art. 6.- El que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema informático, de forma temporal o permanente, será sancionado con prisión de tres a cinco años.

Se considerará agravada la interferencia o alteración, si ésta recayera en programas o sistemas informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión y transporte de energía, de medios de transporte u otros de servicio público, o destinados a la prestación de servicios financieros, la sanción de prisión será de tres a seis años.

Daños a Sistemas Informáticos

Art. 7.- El que destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático que utilice las Tecnologías de la

Información y la Comunicación o cualquiera de los componentes que las conforman, será sancionado con prisión de tres a cinco años.

Si el delito previsto en el presente artículo se cometiere de forma culposa, por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, será sancionado con prisión de uno a tres años.

Si el delito previsto en el presente artículo se cometiere en contra de cualquiera de los componentes de un sistema informático que utilicen las Tecnologías de la Información y la Comunicación, que estén destinadas a la prestación de servicios públicos o financieros, o que contengan información personal, confidencial, reservada, patrimonial, técnica o propia de personas naturales o jurídicas, la sanción de prisión será de tres a seis años.

Posesión de Equipos o Prestación de Servicios para la Vulneración de la Seguridad

Art. 8.- El que utilizando las Tecnologías de la Información y la Comunicación posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente Ley, será sancionado con prisión de tres a cinco años.

Violación de la Seguridad del Sistema

Art. 9.- La persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionado con prisión de tres a seis años.

En igual sanción incurrirá quien induzca a un tercero para que de forma involuntaria, ejecute un programa, mensaje, instrucciones o secuencias para violar medidas de seguridad.

No incurrirá en sanción alguna quien ejecute las conductas descritas en los Arts. 8 y 9 inciso primero de la presente Ley, cuando con autorización de la persona facultada se realicen acciones con el objeto de conducir pruebas técnicas o auditorías de funcionamiento de equipos, procesos o programas.

Estafa informática

Art. 10.- El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco años.

Se sancionará con prisión de cinco a ocho años, si las conductas descritas en el inciso anterior se cometieren bajo los siguientes presupuestos:

a) En perjuicio de propiedades del Estado;

b) Contra sistemas bancarios y entidades financieras; y,

c) Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos.

Fraude Informático

Art. 11.- El que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de tres a seis años.

Espionaje Informático

Art. 12.- El que con fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años.

Si alguna de las conductas descritas en el inciso anterior se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas, resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión.

Hurto por Medios Informáticos

Art. 13.- El que por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado con prisión de dos a cinco años.

Técnicas de Denegación de Servicio

Art. 14.- El que de manera intencionada, utilizando las técnicas de la denegación de servicio o prácticas equivalentes que afectaren a los usuarios que tienen pertenencia en el sistema o red afectada, imposibilite obtener el servicio, será sancionado con prisión de tres a cinco años.

Manipulación de Registros

Art. 15.- Los Administradores de las Plataformas Tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en un registro de acceso, uso de los componentes de éstos, será sancionado con prisión de cinco a ocho años.

Si las conductas descritas en el inciso anterior, favorecieren la comisión de otro delito, la sanción se agravará hasta en una tercera parte del máximo señalado.

Manipulación Fraudulenta de Tarjetas Inteligentes o Instrumentos Similares

Art. 16.- El que intencionalmente y sin la debida autorización por cualquier medio cree, capture, grabe, copie, altere, duplique, clone o elimine datos informáticos contenidos en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; con el objeto de incorporar, modificar usuarios, cuentas, registros, consumos no reconocidos, la configuración actual de éstos o de los datos en el sistema, será sancionado con prisión de cinco a ocho años.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores adquiera, comercialice, posea, distribuya, venda, realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos

destinados al mismo fin o de datos informáticos contenidos en ellos o en un sistema.

Obtención Indebida de Bienes o Servicios por Medio de Tarjetas Inteligentes o Medios Similares

Art. 17.- El que sin autorización utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, utilice indebidamente las Tecnologías de la Información y la Comunicación para la obtención de cualquier bien o servicio, realice cualquier tipo de pago sin erogar o asumir obligación alguna por la contraprestación obtenida, será sancionado con prisión de tres a ocho años.

Provisión Indebida de Bienes o Servicios

Art. 18.- El que sin justificación, a través de un sistema informático utilice tarjetas inteligentes o instrumentos similares destinados a los mismos fines, cuya vigencia haya caducado o haya sido revocada por la institución que la emitió, o que se haya obtenido con el fin de suplantar la identidad contenida en dichas tarjetas inteligentes, será sancionado con prisión de cinco a ocho años.

El que falsifique o altere los datos de las tarjetas inteligentes o instrumentos similares, con el fin de proveer a quien los presente, dinero, bienes o servicios, o cualquier otro objeto de valor económico, la sanción aumentará hasta una tercera parte del máximo de la pena prevista en el inciso anterior.

Alteración, Daño a la Integridad y Disponibilidad de los Datos

Art. 19.- El que violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en

cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento, será sancionado con prisión de tres a seis años.

Interferencia de Datos

Art. 20.- El que interfiera, obstruya o interrumpa el uso legítimo de datos o los produzca nocivos e ineficaces, para alterar o destruir los datos de un tercero, será sancionado con prisión de tres a seis años.

Si alguna de las conductas descritas en el inciso anterior recae sobre datos, documentos, programas o sistemas informáticos públicos o sobre datos destinados a la prestación de servicios de salud, de comunicaciones, sistemas bancarios, entidades financieras, de provisión y transporte de energía, de medios de transporte u otro servicio público, la sanción de prisión será de cinco a ocho años.

Interceptación de Trasmisiones entre Sistemas de las Tecnologías de la Información y la Comunicación

Art. 21.- La persona que sin justificación intercepte por medios tecnológicos cualquier transmisión hacía, desde o dentro de un sistema informático que no está disponible al público; o las emisiones electromagnéticas que están llevando datos de un sistema informático, será sancionado con prisión de siete a diez años.

Hurto de Identidad

Art. 22.- El que suplantare o se apoderare de la identidad de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años.

Si con la conducta descrita en el inciso anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para sí mismo o para terceros y el apoderamiento recae

sobre datos personales, confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública, será sancionado con prisión de cinco a ocho años.

Divulgación No Autorizada

Art. 23.- El que sin autorización da a conocer un código, contraseña de acceso o cualquier otro medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse así mismo, a un tercero o para cometer un delito, será sancionado con prisión de cinco a ocho años.

Igual sanción tendrá el que sin autorización revele o difunda los datos o información, contenidos en un sistema informático que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, con el fin de obtener algún tipo de beneficio para sí o para otro.

Si alguna de las conductas descritas en los incisos anteriores pusieren en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado, será sancionado con prisión de seis a doce años.

Utilización de Datos Personales

Art. 24.- El que sin autorización utilice datos personales a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, será sancionado con prisión de cuatro a seis años.

La sanción aumentará hasta en una tercera parte del máximo de la pena prevista en el inciso anterior a quien proporcione o revele a otro, información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar.

Obtención y Transferencia de Información de Carácter Confidencial

Art. 25.- El que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años.

Revelación Indebida de Datos o Información de Carácter Personal

Art. 26.- El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años.

Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años.

Se impondrá el límite máximo de la pena del inciso anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos

personales confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública.

Acoso a través de Tecnologías de la Información y la Comunicación

Art. 27.- El que realice conducta sexual indeseada por quien la recibe, que implique frases, señas u otra conducta inequívoca de naturaleza o contenido sexual, por medio del uso de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de cuatro a seis años.

Pornografía a través del Uso de Tecnologías de Información y la Comunicación.

Art. 28.- El que por cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación fabrique, transfiriera, difunda, distribuya, alquile, venda, ofrezca, produzca, ejecute, exhiba o muestre material pornográfico, sexual entre niñas, niños y adolescentes o personas con discapacidad, será sancionado con prisión de cuatro a ocho años.

Quien no advierta de forma visible el contenido del material pornográfico o sexual que se transmita mediante el uso de las Tecnologías de la Información y la Comunicación, no apto para niñas, niños, adolescentes o personas con discapacidad, será sancionado con prisión de tres a cinco años.

Utilización de Niñas, Niños, Adolescentes o Personas con Discapacidad en Pornografía a través del Uso de las Tecnologías de la Información y la Comunicación

Art. 29.- El que por cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación produzca, reproduzca,

distribuya, publique, importe, exporte, ofrezca, financie, venda, comercie o difunda de cualquier forma, imágenes, videos o exhiba en actividades sexuales, eróticas o inequívocas de naturaleza sexual, explícitas o no, reales o simuladas, o utilice la voz de niñas, niños, adolescentes o personas con discapacidad, será sancionado con prisión de ocho a doce años.

Igual sanción se impondrá a quien por medio de las Tecnologías de la Información y la Comunicación organice o participe en espectáculos públicos o privados, en los que se hace participar a las personas señaladas en el inciso anterior, en acciones pornográficas o eróticas.

Adquisición o Posesión de Material Pornográfico de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación

Art. 30.- El que adquiera para sí o para un tercero a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, o posea material pornográfico en el que se haya utilizado a una niña, niño, adolescente o persona con discapacidad o su imagen para su producción, será sancionado con prisión de dos a cinco años.

Igual sanción se aplicará al que posea en dispositivos de almacenamiento de datos informáticos o a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, material pornográfico en el que se haya utilizado a una niña, niño, adolescente o persona con discapacidad o su imagen para su producción.

Corrupción de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación

Art. 31.- El que mantenga, promueva o facilite la corrupción de una niña, niño, adolescente o persona con discapacidad con fines eróticos, pornográficos u obscenos, por medio de las Tecnologías de la Información y la Comunicación, aunque la niña, niño, adolescente o persona con discapacidad lo consienta, será sancionado con prisión de ocho a doce años.

Igual sanción se impondrá a quien haga propuestas implícitas o explícitas para sostener encuentros de carácter sexual o erótico, o para la producción de pornografía a través del uso de las Tecnologías de la Información y la Comunicación para sí, para otro o para grupos, con una niña, niño, adolescente o persona con discapacidad.

Acoso a Niñas, Niños y Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación

Art. 32.- Quien atormente, hostigue, humille, insulte, denigre u otro tipo de conducta que afecte el normal desarrollo de la personalidad, amenace la estabilidad psicológica o emocional, ponga en riesgo la vida o la seguridad física, de un niño, niña, adolescente o persona con discapacidad, por medio del uso de las Tecnologías de la Información o Comunicación, será sancionado con prisión de dos a cuatro años.

La pena se agravará con prisión de cuatro a ocho años, para quien realice conducta que implique frases, señas u otra acción inequívoca de naturaleza o contenido sexual contra una niña, niño, adolescente o persona con discapacidad, por medio del uso de las Tecnologías de la Información y la Comunicación.

Suplantación en Actos de Comercialización

Art. 34.- El que sin autorización y a nombre de un tercero, mediante el uso de las Tecnologías de la Información y la Comunicación, venda o comercialice bienes o servicios, suplantando la identidad del productor, proveedor o distribuidor autorizado, será sancionado con prisión de tres a cinco años.

La conducta descrita en el inciso anterior se agravará con pena de prisión de cuatro a seis años, cuando la venta o comercialización se trate de medicamentos, suplementos o productos alimenticios, bebidas o cualquier producto de consumo humano.

1.4.2.3 Código Penal

Pornografía

Art 172.- El que por cualquier medio directo, inclusive a través de medios electrónicos, fabricare, transfiriere, difundiere, distribuyere, alquilare, vendiere, ofreciere, produjere, ejecutare, exhibiere o mostrare, películas, revistas, pasquines o cualquier otro material pornográfico entre menores de dieciocho años de edad o persona con discapacidad intelectual, será sancionado con prisión de tres a cinco años.

en la misma sanción incurrirá el que no advirtiere, de forma visible, sobre el contenido de las películas, revistas, pasquines o cualquier otro material, inclusive el que se pueda transmitir a través de medios electrónicos, cuando éste fuere inadecuado para menores de dieciocho años de edad o persona con discapacidad intelectual.

Utilización de personas menores de dieciocho años e incapaces o deficientes mentales en pornografía.

Art. 173.- El que produzca, reproduzca, distribuya, publique, importe, exporte, ofrezca, financie, venda, comercie o difunda de cualquier

forma, imágenes, utilice la vos de una persona menor de dieciocho años, incapaz o deficiente mental, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en el que exhiban, en actividades sexuales, eróticas o inequívocas de naturaleza sexual, explícitas o no, reales o simuladas, será sancionado con prisión de seis a doce años.

Igual sanción se impondrá a quien organizare o participare en espectáculos, públicos o privados, en los que se hace participar a las personas señaladas en el inciso anterior, en acciones pornográficas o eróticas.

Posesión de pornografía.

Art. 173-A.- El que posea material pornográfico en el que se utilice la imagen de personas menores de dieciocho años, incapaces o deficientes mentales, en actividades pornográficas o eróticas, será sancionado con pena de dos a cuatro años.

Violación de comunicaciones privadas

Art. 184.- El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa.

El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

Violación agravada de comunicaciones

Art. 185.- Si los hechos descritos en el artículo anterior se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo público de seis meses a dos años.

Estafa agravada

Art. 216.- El delito de estafa será sancionado con prisión de cinco a ocho años, en los casos siguientes: (…)

5) Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos.

Daños agravados

Art. 222.- Se impondrá prisión de dos a cuatro años: (…)

2) Si el daño se realizare mediante manipulación informática.

Infidelidad comercial

Art. 230.- El que se apoderare de documentos, soporte informático u otros objetos, para descubrir o revelar un secreto evaluable económicamente, perteneciente a una empresa y que implique ventajas económicas, será castigado con prisión de seis meses a dos años.

1.4.2.4 Código Procesal Penal

Obtención y reguardo de información electrónica

Art 201.- cuando se tenga razones fundadas para inferir que una persona posee información constitutiva de delito o útil para la investigación, almacenada en equipos o instrumentos tecnológicos de su propiedad o posesión, el fiscal solicitara la autorización judicial para adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información; sin perjuicio que se ordene el secuestro respectivo.

CAPITULO II

EL DELITO INFORMATICO Y SU REALIDAD PROCESAL EN EL SISTEMA PENAL SALVADOREÑO.

2.1 SINTESIS DEL PROBLEMA

CODIGO	TEMA FUNDAMENTAL	CATEGORIAS BASICAS
01	Delitos comunes cometidos mediante sistemas informáticos regulados en la LECDIC.	✓ LECDIC
02	El proceso investigativo: Investigación tecnológica de los delitos informáticos.	✓ Constitución de la Republica ✓ Código procesal penal
03	Limitaciones del Sistema Penal para la Investigación de los delitos informáticos.	✓ Limitaciones ✓ Delitos Informáticos ✓ LECDIC
04	Desafíos investigativos y procesales del sistema penal para la aplicación de la ley especial contra los delitos informáticos y conexos-	✓ Desafíos ✓ Sistema Penal ✓ Ley especial

2.2 DELITOS COMUNES COMETIDOS MEDIANTE SISTEMAS INFORMATICOS REGULADOS EN LA LECDIC

No todos los delitos que se vieron favorecidos por la invención de la tecnología informática pueden ser considerados como informáticos, por esto estimamos la necesidad de hablar de delitos cometidos a través de medios informáticos (delitos computacionales), que aumentaron sus formas de comisión o que mutaron para lograr mayor eficacia en sus resultados, o simplemente se adaptaron al nuevo medio. Todo delito (a excepción del de propia mano) puede en alguna medida ser realizado

mediante la utilización de un sistema informático, máxime si se encuentra conectado a Internet, rescatamos la convivencia pacífica con el delito informático propiamente dicho, así como el hecho de que comparten algunas similitudes.

Los ilícitos penales descritos a continuación tienen una característica especial, debido a que en El Salvador, la proliferación de internet ha permitido el desarrollo de nuevos modus operandi para la ejecución de actividades criminales como difamación, amenaza, estafa, violación a derechos de autor, distribución de pornografía infantil, robo de identidad, entre otras.

2.2.1 ESTAFA INFORMÁTICA

Art 10.- *El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco años…*

Así pues, estamos ante una figura autónoma respecto de la estafa común, frente a esta, la diferencia sustancial como ya se apuntó, consiste en la ausencia de engaño y error, caracterizándose la estructura típica de la estafa informática por el hecho de que la disposición patrimonial se consigue valiéndose el autor de alguna “operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema…”

- **Bien jurídico.**

Sintéticamente en opinión de Rovira del Canto, “el tipo penal exige la afectación, tanto del patrimonio económico (activos) del sujeto pasivo, como la puesta en peligro de la seguridad de la información informatizada y de las funciones informáticas en sentido estricto. Por esto, se trata de un delito pluriofensivo”.49 (Rovira Canto, 2002, pág. 70) En igual sentido se pronuncia Gutiérrez Francés (1994) al señalar que el bien jurídico tutelado en los delitos informáticos (en general) se concibe en dos planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, patrimonio, entre otros.

- **Sujeto activo.**

Común: “El que” utilizado por el legislador indica que sujeto activo puede ser cualquier persona natural que realice la acción propia del tipo penal, sin que este requiera alguna calificación particular o especial o poseer específicos conocimientos técnicos en materia informática. No se excluye como sujeto activo al titular legítimo del sistema al momento de efectuar una manipulación informática a su favor y en perjuicio de otro. Rovira del Canto, apunta que, generalmente no se puede confundir el sujeto activo del tipo con el beneficiario de la acción criminal, en tanto que, ocasionalmente los beneficiaros no son quienes realizan la conducta punible y, en muchos casos, no es de su conocimiento la acción defraudatoria.50 (Rovira Canto, 2002, pág. 71).

---

49 Rovira Canto, E. (2002). **Delincuencia Informática y Fraudes Informáticos**. Granada: Comares. Pág. 70

50 Ibídem Pág. 71

- **Sujeto pasivo.**

Común: sujetos pasivos del delito son además del titular del derecho patrimonial objeto de afectación, los titulares individuales de la información, de los datos o programas objeto de la acción delictual, y de los equipos y sistemas afectados, aunque no sufran perjuicio económico patrimonial efectivo, así como la sociedad en general en cuanto titular de la información informatizada y de los sistemas por los que se procesa y transfiere. Esto es, solo pueden ser sujetos pasivos de este tipo penal las personas que, por una parte, sean titulares del bien jurídico patrimonio económico perjudicado y de los datos informatizados con valor contable y, por la otra, aquella persona que sea el titular del medio informático que resulta objeto de manipulación por parte del autor, que incluso puede ser una persona jurídica (instituciones crediticias, gobiernos, empresas, entre otros) que utilizan sistemas automatizados de información, generalmente conectados a otros.

- **Conducta típica.**

La conducta típica se consuma ejecutando las siguientes formas de acción en un sistema que utilice las Tecnologías de la Información y la Comunicación, las cuales se definen en el Art. 3 de la LECDIC:

Manipulación.

- ✓ Manipulando o influyendo en el ingreso de los datos (input). Mata Martin, denomina a esta fase Manipulación previa, agregando que, en su ejecución práctica, “la manipulación de carácter previo puede ser activa, en sentido estricto (modificando datos reales o añadiendo otros ficticios). En este caso los datos tratados automáticamente son incorrectos, manteniéndose intacto el programa y siendo correcto el tratamiento o procesamiento de datos. Ejemplo de ello serían la

introducción de nombre de trabajadores falsos en una planilla para que se les hagan pagos inexistentes."[51] (Mata, 2003, pág. 33).

Para la realización de las conductas antes descritas, el sujeto activo deberá valerse de: el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o "artificio" tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro.

2.2.2 FRAUDE INFORMÁTICO

Inicialmente adoptaremos la definición doctrinal sugerida por del Pino, fraude informático es: "el conjunto de conductas dolosas, que, valiéndose de cualquier manipulación fraudulenta, modifiquen o interfieran el funcionamiento de un programa informático, sistema informático, sistema telemático o alguna de sus partes componentes, para producir una ventaja económica ilícita, a favor de su perpetrador o un tercero".[52] (De Pino, 2016, pág. 45).

El fraude informático es calificado como una de las tipologías del cibercrimen en el que se da la defraudación mediante la utilización de un sistema informático como medio para transferir (de forma virtual e inaprensible) activos patrimoniales a favor del autor o de un tercero. También se denomina diversamente como: "estafa telemática", "estafa por computación" (Alemania),"estafa informática" (España, El Salvador), "fraude informático" (Costa Rica, El Salvador).En la LECDIC salvadoreña se tipifican los delitos de Estafa Informática (Art. 10) y Fraude Informático (Art. 11).

---

51 Mata, R. M. (2003). **Delincuencia Informática y Derecho penal**. México: Hispamer.
52 Del Pino, S. A. (18 de 06 de 2016). **Delitos Informáticos. Obtenido de Generalidades**: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.

Art 11.- *"El que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de tres a seis años"."*

- **Bien jurídico.**

Al igual que la estafa el tipo penal exige la afectación, tanto del patrimonio económico (activos) del sujeto pasivo, como la puesta en peligro de la seguridad de la información informatizada y de las funciones informáticas en sentido estricto. Por esto, se trata de un delito pluriofensivo. Es decir, la información de manera general, en referencia a la información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos, y específicamente patrimonio.

- **Sujeto activo.**

Común: "El que" empleado por el legislador implica que cualquier persona natural que realice la acción propia del tipo penal puede ser sujeto activo del tipo, sin que este requiera alguna calificación particular o especial o poseer específicos conocimientos técnicos en materia informática. No se excluye como sujeto activo al titular legítimo del sistema al momento de efectuar una manipulación informática a su favor y en perjuicio de otro.

- **Sujeto pasivo.**

Aplica lo señalado para el delito de estafa Informática.

- **Conducta típica.**

La acción que es punible en este delito se define como una conducta de carácter doloso, siendo el mismo un delito de resultado, donde lo que

se persigue es el “provecho” (beneficio patrimonial o no patrimonial) para sí o para un tercero.

La conducta típica se consuma ejecutando las siguientes formas de acción en un sistema que utilice las Tecnologías de la Información y la Comunicación:

- ✓ El uso indebido de las TIC’s y valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida.
- ✓ Conseguir insertar instrucciones falsas o fraudulentas en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida.

2.2.3 HURTO DE IDENTIDAD

El tipo penal regulado en el art. 22 de la LECDIC dispone lo siguiente:

Art. 22.- *El que suplantare o se apoderare de la identidad de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años.*

Si con la conducta descrita en el inciso anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para sí mismo o para terceros y el apoderamiento recae sobre datos personales, confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública, será sancionado con prisión de cinco a ocho años”.

Se puede afirmar que desde el punto de vista del Derecho “la Identidad hace referencia a un conjunto de características, datos o

informaciones que permiten individualizar a una persona".[53] (Carrasco, 2010, pág. 200).

Al respecto, en relación con la identificación de un imputado en el proceso penal se ha dicho que se debe distinguir entre individualizar e identificar.

De conformidad a la Real Academia Española de la Lengua "individualizar" es sinónimo de "individuar" que significa "Determinar individuos comprendidos en una especie". También es sinónimo de "particularizar" que significa "Extraer una cosa con todas sus circunstancias o particularidades". Por su parte "identificar" es "Reconocer si una persona o cosa es la misma que se expone o busca."

En la actualidad, con el desarrollo y uso de las nuevas tecnologías de la información y de la comunicación (TIC's), se han desarrollado ámbitos de desarrollo de la personalidad en el llamado mundo virtual, a través de medios de comunicación informática, tales como: página de internet o web, correos electrónicos, redes sociales (Facebook, Twitter, Instagram, etc.), y otros, en los que las personas expresan muy frecuentemente ámbitos de su intimidad, por lo que merecen protección jurídica; sin embargo, al igual que ocurre en la identidad física de las personas, que se ha desarrollado ampliamente, para que exista esa protección, es necesario e indispensable que el uso de esos medios de comunicación informática expresen características que permitan identificar al titular de ese derecho a la intimidad, pues si eso no existe -que frecuentemente ocurre por el anonimato que permite en general el internet- tal protección no sería jurídicamente aceptable.

53 Carrasco, L. (2010). **"Casos de Suplantación de Identidad Detectados en Denuncias Tramitadas por la Agencia Española de Protección de Datos"** citado por Marta y Martin, Ricardo en " El robo de Identidad". España: Universidad de Castilla. Pág. 200.

Por ejemplo, si una página de internet identifica claramente las características de su titular -que no sólo es aplicable a personas naturales o físicas, sino también a personas jurídicas-, merece la protección del derecho penal, por ejemplo, la Fiscalía General de la República de El Salvador, cuenta con el dominio http://www.fiscalia.gob.sv/, que la hace absolutamente identificable como titular de la misma, pues se consigna en la misma, el nombre de la institución “fiscalía”, “que se trata de una entidad de gobierno, al utilizar el identificador “Gob.” y que se refiere al Estado de El Salvado, al identificarse con el dominio geográfico “sv”, asignado internacionalmente a El Salvador”.[54] (Colveo, 2017).

El denominado “hurto de identidad”, “usurpación de identidad”, “suplantación de identidad” o “falsificación de la identidad y su uso indebido” de acuerdo con investigaciones internacionales realizadas por el Consejo Económico y Social (ECOSOC) de la Organización de las Naciones Unidas, La Unión Europea y la Organización para la Cooperación y el Desarrollo Económico (OCDE) es “el delito de más rápido crecimiento en el mundo sin que existan acciones legislativas concretas y políticas públicas acertadas para sancionar esta conducta atípica en el plano penal”.55 (Omero Flores, 2016, pág. 851).

Para concluir, vale la pena señalar, que en razón de todo lo expuesto la identidad protegida por este tipo penal, no es la identidad real de la persona, o como se ha expresado, sus generales, que pueden materializarse en documentos de identidad: documento único de identidad, licencia de conducir, pasaporte, número de identificación tributaria y otros; pues los supuestos de afectación de suplantación o apoderamiento de esa

54 Colveo, J. L. (13 de octubre de 2017). **Los Nombres de Dominio. Obtenido de Anetcom Generalitat**: https://www.**filmac.com/wp-conten/uploads/librodominios.**

55 Omero Flores, R. (2016). "Las Conductas vinculadas a la suplantación de identidad por edios telemáticos: una propuesta de acción legislativa". México: Unam. Pág. 851.

identidad deben canalizarse por medio de los tipos penales contenidos en el Código Penal y concretamente el siguiente:

Uso Falso de Documento de Identidad

Art. 288.- El que usare como propio, pasaporte, o cualquier documento de identidad que no le correspondiere legalmente o el que cediere el propio, para que otro lo utilizare indebidamente, será sancionado con prisión de seis meses a un año".

- **Bien jurídico.**

El bien jurídico tutelado por el tipo penal que comentamos, ante estas inéditas conductas desarrolladas por la delincuencia informática, no resulta un tema menor por las graves consecuencias para los ciudadanos que son víctimas del robo de identidad.

Los efectos directos generados por la suplantación o apoderamiento de identidad pueden serlo en varios órdenes:

- ✓ En principio pueden ser daños fundamentalmente económicos o patrimoniales, si la identidad suplantada o de la cual se han apoderado, es utilizada para actividades comerciales en internet, tales como la imputación de ciertos gastos y operaciones comerciales a quien aparece falsamente como titular de los datos contractuales, [56] (Carrasco, 2010, pág. 73) que inclusive puede derivarse en la negación al pago de una operación que realmente no ha llevado a cabo y la inevitable producción de efectos sobre su reputación financiera, esto es, el ciudadano suplantado tiene inicialmente un daño patrimonial.

56 Carrasco, L. (2010). "**Casos de Suplantación de Identidad Detectados en Denuncias Tramitadas por la Agencia Española de Protección de Datos"** citado por Marta y Martin, Ricardo en " El robo de Identidad". España: Universidad de Castilla. Pág. 73.

- ✓ Sin embargo, a la usurpación de identidad le suceden una cascada de perjuicios de distinta naturaleza que podrían incluir ataques a la privacidad o intimidad de las personas y daños de tipo psicológico.

- ➢ **Sujeto activo.**

Común: “El que”: cualquier persona natural que realice la acción propia del tipo penal, pues el tipo no requiera alguna calidad, condición o calificación particular o especial o poseer específicos conocimientos técnicos en materia informática por parte del actor, sin embargo en atención a que ciertas técnicas utilizadas para la consumación del delito, requieren de específicos conocimientos técnicos en materia informática por parte del sujeto activo, es inevitable tener en cuenta dicha calificación al momento de definir un caso concreto.

- ➢ **Sujeto pasivo.**

Común: sujetos pasivos de la suplantación o apropiación de identidad informática puede ser como lo señala expresamente el tipo penal cualquier persona natural (o física) o persona jurídica que sea titular de la protección a su intimidad, privacidad o patrimonio en los términos señalados supra.

2.2.4 UTILIZACIÓN DE DATOS PERSONALES

El tipo penal regulado en el art. 24 de la LECDIC dispone lo siguiente:

Art. 24.- *El que sin autorización utilice datos personales a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando modificando los datos en perjuicio de un tercero, será sancionado con prisión de cuatro a seis años.*

La sanción aumentará hasta en una tercera parte del máximo de la pena prevista en el inciso anterior a quien proporcione o revele a otro,

información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar.

- **Bien jurídico.**

El legislador salvadoreño colocó este tipo penal en el capítulo que ha denominado “Delitos Informáticos relacionados con el contenido de los datos”, y es de los tipos penales de la LECDIC que menciona en su redacción al contenido de la información (los datos informáticos) como objeto de protección, por lo que se puede señalar que el bien jurídico tutelado en consecuencia, se puede comenzar a sostener que estamos en presencia de un valor social que necesita la protección del derecho y en particular del derecho penal, que se ha categorizado como la “integridad de los sistemas y datos informáticos”.

No obstante, lo anterior, en virtud que además se sanciona el uso ilegitimo de los datos personales obtenidos es posible vincularlo con el derecho a la intimidad, materializado en el contenido de los datos informáticos, por lo que se puede hablar de un tipo penal pluriofensivo, entre el derecho a la intimidad y la mencionada integridad de sistemas y datos informáticos.

- **Sujeto activo.**

Común: La fórmula utilizada por el legislador consistente en “El que sin autorización”, indica que puede ser sujeto activo cualquier persona natural que realice la acción propia del tipo penal.

- **Sujeto pasivo.**

Común: Pueden ser sujetos pasivos del tipo penal cualquier persona natural o jurídica que sea titular de la información personal que se divulgue.

- **Conducta típica.**

La parte objetiva de la conducta típica comprende aquella que "utilice datos personales a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando modificando los datos en perjuicio de un tercero".

2.2.5 REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER PERSONAL

El tipo penal regulado en el art. 26 de la LECDIC dispone lo siguiente:

Art. 26.- *El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años.*

Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años.

Se impondrá el límite máximo de la pena del inciso anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos personales confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública".

- **Bien jurídico.**

El legislador salvadoreño colocó este tipo penal en el capítulo que ha denominado "Delitos Informáticos relacionados con el contenido de los

datos”, y es de los tipos penales de la LECDIC que menciona en su redacción al contenido de la información (los datos informáticos) como objeto de protección, por lo que podemos señalar que el bien jurídico tutelado en consecuencia, se puede comenzar a sostener que estamos en presencia de un valor social que necesita la protección del derecho y en particular del derecho penal, que se ha categorizado como la “integridad de los sistemas y datos informáticos”.

No obstante, lo anterior, en virtud que además se sanciona la difusión o cesión de información de carácter privada y personal es posible vincularlo con el derecho a la intimidad, materializado en el contenido de los datos informáticos, por lo que se puede hablar de un tipo penal pluriofensivo, entre el derecho a la intimidad y la mencionada integridad de sistemas y datos informáticos.

- **Sujeto activo.**

Común: En virtud de la formulación utilizada por el legislador, consistente en “El que sin el consentimiento”, podemos concluir que se trata de un delito común, en el cual el sujeto activo no debe contar con ninguna cualidad o calidad especial, por lo que puede ser realizado por cualquier persona natural.

- **Sujeto pasivo.**

Común: Puede ser sujeto pasivo cualquier persona natural o jurídica titular de la información de carácter privada y personal.

- **Conducta típica.**

La parte objetiva de la conducta típica comprende el que “sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto,

audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes".

2.2.6 ACOSO A TRAVÉS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

El tipo penal regulado en el art. 27 de la LECDIC dispone lo siguiente:

"Acoso a través de Tecnologías de la Información y la Comunicación

Art. 27.- El que realice conducta sexual indeseada por quien la recibe, que implique frases, señas u otra conducta inequívoca de naturaleza o contenido sexual, por medio del uso de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de cuatro a seis años".

- **Bien jurídico.**

Se refiere a la libertad sexual exclusivamente pues se refiere a conductas realizadas en víctimas mayores de 18 años, pues de ser niñas, niños o adolescentes, ello se tipifica en el inciso segundo del art. 32 de la misma LECDIC.

Se entiende por libertad sexual "la capacidad cognoscitiva y valorativa del sujeto pasivo, referida al significado y trascendencia del acto sexual, así como del consentimiento que, eventualmente, pueda prestar a él. De ello se deriva que, donde falte esa capacidad, faltará también la libertad sexual, que por tanto no puede ser violada o menoscabada".

"Por consiguiente, la libertad sexual no es aplicable para aquellas personas que el ordenamiento jurídico considera que carecen total o parcialmente, de manera temporal o permanente de tal capacidad; estamos en los supuestos de incapacidad legal, tales como la minoría de edad, la enajenación mental o la deficiencia mental. En estos casos, la doctrina en general ha considerado que lo protegido es la indemnidad

sexual”; lo que sería replicable respecto del inciso segundo del art. 32 de la LECDIC.

- **Sujeto activo**

Común: Con la redacción utilizada por el legislador “El que”, se indica que puede ser cualquier persona natural que realice la acción propia del tipo penal.

- **Sujeto pasivo.**

Común: Puede ser sujeto pasivo cualquier persona, hombre o mujer

- **Conducta típica**.

La parte objetiva de la conducta típica comprende frases, señas u otra conducta inequívoca de naturaleza sexual transmitidas al sujeto pasivo por medio de la TIC´s.

2.3 IDENTIDICACION DE CASOS PRACTICOS

Del 06 de marzo de 2016 al 30 de junio de 2019

DELITOS LECDIC	Estafa Informática Art.10 Lit. a	Fraude Informático Art 11.	Hurto de Identidad. Art 22	Utilización de datos personales. Art 24	Revelación Indebida de Datos o información de carácter personal. Art 26	Acoso a través de Tecnologías de la Información y la Comunicación. Art 27	Total de Casos Denunciados
NUMERO DE CASOS							
Cantidad de Casos	11	13	119	95	243	55	536
ESTADO DEL PROCESO							
Archivo Provisional	0	0	0	2	0	1	
Archivo Definitivo	1	2	22	25	47	13	
Expediente Activo	10	13	97	68	196	41	
Total	**11**	**13**	**119**	**95**	**243**	**55**	**536**

2.4 EL PROCESO INVESTIGATIVO DE LOS DELITOS INFORMÁTICOS

El proceso investigativo en los delitos informáticos permite la aplicación de todas las diligencias reguladas en el CPP, así como los diversos actos urgentes de comprobación.

Sin embargo, deben estimarse la diferencias sustanciales de los delitos informáticos y los demás delitos, en relación con las evidencias, mientras en los delitos tradicionales la evidencia generalmente cuenta con un carácter material o corpóreo, las evidencias digitales carecen de él, y se mantienen dentro de soportes que los contienen, pero que no los sustituyen, por ejemplo el contenido de un correo electrónico, una imagen o un video, puede estar archivado en un disco compacto, un DVD, una memoria USB, la memoria interna de un teléfono celular, una Tablet, el disco duro de una computadora u otro dispositivo de almacenamiento, pero estos no los sustituyen, sino que sólo los soportan.

2.4.1 Obtención, resguardo y/o almacenamiento de la información

Por ello el acceder a esta información debe partir de cumplir con el principio de legalidad, y al tener contacto inicial con una investigación de delitos informáticos el asegurar la información debe cumplir con lo dispuesto en el art. 201 del CPP., que dispone lo siguiente:

“Obtención y resguardo de información electrónica

Art. 201.- *Cuando se tengan razones fundadas para inferir que una persona posee información constitutiva de delito o útil para la investigación, almacenada en equipos o instrumentos tecnológicos de su propiedad o posesión, el fiscal solicitará la autorización judicial para adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información; sin perjuicio que se ordene el secuestro respectivo.*

“Durante dispositivos de entrega bajo cobertura policial, operaciones policiales encubiertas, allanamientos, requisas penitenciarias o de cualquier lugar de detención y en los casos de flagrancia previa dirección funcional de la Fiscalía General de la República, la policía podrá adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información almacenada en equipos o instrumentos tecnológicos y que sea útil para la investigación, sin perjuicio de que pueda procederse a su incautación.”

En ambos supuestos la validación legal es para obtener, resguardar o almacenar la información contenida en equipos o instrumento tecnológicos.

En resumen se trata de acciones orientas a extraer del dispositivo -no a vaciar, sin eliminarlo del equipo dispositivo de almacenamiento que lo contiene -porque esa se constituye en la evidencia digital original-, información o los datos informáticos que contiene; es decir se trata de obtener una copia integral de la información contenida en el equipo incautado, que se convierte en evidencia digital, y en consecuencia, se transforma en el material de trabajo sobre el cual se realizarán las pericias que correspondan, mientras que se conservan integralmente y sin alteración los archivos digitales originales, contenidos en el equipo del cual fueron extraídos.

En este punto cabe recalcar, que las habilitaciones del art. 201 CPP., para la limitación del derecho a la intimidad, tanto en el supuesto del inciso primero, como de la reciente modificación del inciso segundo, sólo son a efecto de obtener, resguardar o almacenar información o datos informáticos contenidos en dispositivos de almacenamiento; sin embargo, consideramos que las habilitaciones del inciso segundo sólo son justificadas por la urgencia de realizar esa acción, en otras palabras, si no hay urgencia, esa medida no es justificada sin orden judicial, ello en virtud

de constituirse como actos de suma, grave o extrema urgencia, que si no se realizan se perdería información valiosa para una investigación penal y futuro ejercicio de la acción penal.

Lo anterior sería aplicable, sólo en supuestos del hallazgo e incautación de equipos informáticos que se encuentren encendidos y que permitan el almacenamiento de información, pues en la memoria RAM en el caso de computadoras, o similares en tablets o teléfonos celulares, de apagarse o descargarse, se puede perder información útil para la investigación; a contrario sensu, en el caso de equipos informáticos apagados, siempre es posible obtener la autorización judicial para limitar el derecho a la intimidad.

Para realizar actividades de investigación o periciales que consisten en lo que se ha entendido por acceder, registrar o analizar la información o datos informáticos obtenidos, dado que no hay disposición legal expresa, es necesario recurrir al principio de libertad probatoria (art. 176 CPP.), y en consecuencia recurrir a la regulación de los medios de prueba semejantes; se trata de la regulación del registro y allanamiento (art. 191 CPP.), ello por el derecho a la intimidad presente tanto en la información o datos informáticos como en la morada, esto es, que se debe exigir la habilitación por orden judicial para realizar esos procedimientos y poder incorporar sus resultados al proceso penal.

Consecuencia de lo señalado es que las autoridades policiales, incluidas las fuerzas armadas que participan en acciones de seguridad pública, y las fiscales, no cuentan con habilitación legal para que al incautar un equipo informático o dispositivo de almacenamiento de la información en cualquier procedimiento, sin orden judicial, accedan al contenido de información o de datos informáticos; pues eso constituye una vulneración al derecho a la intimidad, que como se ha señalado por principio de libertad probatoria, exclusivamente pueda ser limitado por

orden judicial. Resultado de una práctica como esa, es la existencia de una posible prueba ilícita, que permita en el proceso penal solicitar la exclusión probatoria de toda la evidencia digital contenida en el equipo informático o dispositivo de almacenamiento de la información.

2.4.2 Cadena de custodia de la evidencia en los delitos informáticos

La cadena de custodia es la garantía del justiciable que los objetos o documentos que se incorporen en la vista pública para probar los hechos que se le acusan, son los mismos que fueron incautados en algún momento procesal y que de haberse modificado o cambiado es por razones legales o técnicas.

La modificación o cambio puede ocurrir en virtud de la realización de una pericia, por ejemplo si en una escena del delito se encontró un arma de fuego, de la cual se brindan sus características en el acta correspondiente y se señala que no tiene serie visible, pero que se le ordena una pericia de restauración del número y ello se realiza parcial o totalmente, con lo cual al juicio llega un arma con un número de serie identificador que no se tenía al momento de la incautación, pero se trata del mismo objeto.

La regla de la cadena custodia se regula en el CPP en las siguientes disposiciones:

"Cadena de custodia

Art. 250.- La cadena de custodia es el conjunto de requisitos que, cuando sea procedente, deben observarse para demostrar la autenticidad de los objetos y documentos relacionados con un hecho delictivo.

Aplicación

Art. 251.- Las personas que hayan tenido contacto con los objetos y documentos incautados o recolectados registrarán toda la información necesaria para facilitar la constatación de autenticidad de los mismos en

las diferentes etapas de su manejo o utilización, tales como recolección, embalaje, transporte, análisis y custodia. El defensor o el querellante podrán solicitar el auxilio judicial necesario para que la policía aplique cadena de custodia cuando encontraren objetos o documentos sujetos a tales requisitos.

Legalidad de la cadena de custodia

Art. 252.- Si alguna de las partes impugna de manera fundada la cadena de custodia, la parte interesada en la admisión del objeto o documento deberá demostrar su integridad. Por regla general no estarán sujetos a cadena de custodia los objetos que posean características propias, que los diferencien de manera inequívoca de otros de su misma especie. La interrupción de la cadena de custodia será valorada por el juez.

Regulación que es aplicable a la evidencia digital, cadena que inicia al momento de la incautación, por lo que lo señalado en el número anterior respecto del acceso, registró y análisis de la información forma parte de esta cadena de custodia.

Es importante destacar, que en virtud que técnicamente, los equipos informáticos y dispositivos de almacenamiento de información, están en su mayoría diseñados para registrar en la llamada metadata[57] de los archivos que contienen la información o datos informáticos, es factible a través de pericias determinar cuándo ocurrió el último acceso o modificación de los mismos; ello conlleva a que un perito puede determinar esa información y con ello permitir el cotejo con el día y hora en que la incautación ocurrió, expresado en las actas correspondientes levantadas por las mismas autoridades policiales o fiscales y con ello evidenciar que estando esos

57 Metadata: «**datos estructurados y codificados que describen características de instancias conteniendo informaciones para ayudar a identificar, descubrir, valorar y administrar las instancias descritas».** Traducción libre de W. R. Durrell. Data Administration. A Practical Guide to Data Administration. McGraw-Hill, 1985. Para más información sobre este aspecto técnico, se debe consultar el Manual Técnico respectivo.

equipos o dispositivos en manos de ellas, sucedió un acceso ilegal a tal información y con ello, cuando menos configurar un cuestionamiento a la legalidad de la prueba.

2.4.3 Peritajes en los delitos informáticos

Los peritajes en los delitos informáticos están sujetos a las mismas reglas generales por lo cual es aplicable lo regulado de los artículos 226 a 241 CPP.

Resulta particularmente aplicable lo relacionado con la clase de peritos, es decir permanentes y accidentales, y dentro de los primeros no existe ningún obstáculo para ofrecer inclusive profesionales o técnicos especializados que laboren para la Fiscalía General de la República, pues así lo permite el art. 226, particularmente en la letra c), como especialistas de las instituciones del Estado, pues el Ministerio Público y con la Fiscalía General de la República se encuentran integrados.

2.4.3.1 Nombramiento de Peritos

Clasificación

Art. 226.- El juez o tribunal ordenará peritajes, cuando para descubrir o valorar un elemento de prueba, sea necesario o conveniente poseer conocimientos especiales en alguna ciencia, arte o técnica. En los actos urgentes de comprobación que no requieran autorización judicial el fiscal podrá disponer el auxilio de peritos. Los peritos serán de dos clases: Permanentes o accidentales.

Son peritos permanentes:

a) Los nombrados por la Corte Suprema de Justicia en el Instituto de Medicina Legal o en cualquier otra dependencia de la misma.

b) Los técnicos y especialistas de la Policía Nacional Civil.

c) Los especialistas de las facultades y escuelas de la Universidad de El Salvador y de las dependencias del Estado e instituciones oficiales autónomas.

d) Los directores o jefes de los centros asistenciales del Estado o los que aquéllos designen.

e) Los miembros de cualquier asociación o institución cuya finalidad sea el estudio o análisis de la medicina legal y de las ciencias forenses, que desempeñen algún cargo o empleo público.

Son peritos accidentales los que nombre la autoridad judicial para una pericia determinada.

En el caso de los peritos permanentes no será necesaria su juramentación o protesta para la práctica de las diligencias; su salario habitual serán sus honorarios y la institución para la cual trabajan estará obligada a conceder el permiso para la pericia".

2.5 LIMITACIONES DEL SISTEMA PENAL PARA LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS

El medio electrónico se ha convertido en un blanco para cometer diferentes actos ilegales tales como: extorción, robo, fraude, suplantación de identidad, entre otros. En el ámbito de la delincuencia informática se presentan sin duda importantes complicaciones para el descubrimiento y la investigación de los hechos en y mediante el ordenador, de forma que puede en ocasiones no ser raro que muchos de los casos no lleguen nunca a detectarse.

La investigación de la delincuencia informática, no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios.

Los investigadores de delitos cibernéticos buscan vestigios digitales que de acuerdo a sus características suelen ser volátiles y de vida corta. Es preciso considerar que el internet brinda grandes beneficios a los

usuarios, pero su fácil acceso también podría perjudicarlos. En El Salvador como en cualquier parte del mundo los usuarios de Internet corren un alto riesgo de ser perjudicados mediante actos delictivos relacionado con las tecnologías.

El Salvador por el escaso desarrollo de la investigación y procesamiento de casos, al principio después de la vigencia de la LECDIC no existían muchos casos en que se haya pronunciado sobre la aplicación de la Ley en esta clase de delito, esto debido a la falta de denuncia por parte de la población, es así que durante el año 2016 se denunciaron o aperturaron 144 casos, y en el tiempo transcurrido de 2017, se han abierto 88 casos de los diversos delitos informáticos.

Lo anterior indica una probable evolución en la conciencia de los ciudadanos residentes en el país sobre la existencia de delitos informáticos, y principalmente aquellos que atentan contra la intimidad, el honor y la seguridad de datos informáticos, como son (hurto de identidad, revelación indebida de datos o información de carácter personal y utilización de datos personales) y así denunciar estos delitos.

Entre todas las acciones reportadas a la FGR representan para el año 2016 el 56.25 % son 81 de 144 casos registrados en todo el año, por su parte en el tiempo transcurrido para el informe estadístico en el año 2017, esos delitos representan el 63.09% se trata de 53 de 84 casos abierto en la FGR y contabilizando desde el año 2016 hasta el 30 de Junio del año 2019 el 72.20 % son 387 de 536 casos abierto en la FGR. Si adicionalmente se observa el estado del proceso se demuestra que aún hay poco ejercicio de la acción penal, para los delitos expresados pues la mayoría se encuentra activos, y en investigación.

Lo anterior conlleva a que aún no hay suficiente experiencia judicial en la aplicación de la ley, por lo que debe esperarse el tratamiento que se

le da a la evidencia digital, la cadena de custodia y la probable consecuencia de ilicitud probatoria en los tribunales de justicia.

2.5.1 Limitantes para el manejo de delitos informáticos

- Falta de la infraestructura y tecnologías adecuada en los entes u organismos de investigación como: el Ministerio de Justicia y Seguridad Publica, la PNC. Las investigaciones o experticias a nivel informático en su mayoría se dan por denuncias realizadas bajo otro contexto de delitos tales como: robo, daño a la propiedad, estafas, entre otros, que son llevadas por las distintas unidades del Ministerio de Justicia y Seguridad Publica que opere este tipo de infracciones.

- Falta de iniciativas que permitan el desarrollo de brigadas y unidades estructuradas y especializadas, (por ejemplo la FGR no cuenta con una Unidad Especial) para la investigación de los delitos de índole informático, nacional y transnacional, desde su inicio con el levantamiento de evidencias hasta la aplicación de procedimientos de mayor complejidad.

- Falta de un procedimiento adecuado para la calificación de peritos informáticos por parte de la Superintendencia del Sistema Financiero y el Ministerio de Justicia y Seguridad Publica.

Otro aspecto, a considerar es la problemática legal, que se presenta cuando este tipo de delitos traspasa las fronteras y las jurisdicciones, lo que pone en relieve la importancia de la cooperación internacional.

2.5.2 Limitaciones de formación

La formación surge como factor incluyente para cada uno de los involucrados que dirigen la investigación, pues muchas veces se encuentran confundidos ante el tratamiento de este tipo de delitos.

- Falta de preparación para los miembros de los organismos que persiguen la delincuencia en el campo informático (Ministerio de Justicia y Seguridad Publica, la PNC, jueces, etc.).
- Falta de preparación a nivel de formación en el ámbito de los procedimientos y técnicas utilizadas para la persecución de los delitos informáticos por parte de los especialistas.
- Falta de programas de capacitación que estén relacionados con los delitos informáticos.
- Falta de cultura informática, aquellas personas que no tienen conocimientos informáticos básicos (Internet, correo electrónico), son más vulnerables y tienen mayores probabilidades de ser víctimas de un delito.

2.5.3 Limitaciones Tecnológicas

Alrededor del mundo existe una amplia diferencia en la distribución de las tecnologías de la información y las comunicaciones, lo que lleva a que existan grandes brechas en los tipos y números de adelantos tecnológicos entre los países. De esta situación surge lo que hoy día se conoce como brecha digital, la cual fue reconocida desde la declaración del milenio hecha por las Naciones Unidas en el año 2000.

La brecha digital hace referencia a las desigualdades en el acceso a internet, nuevas tecnologías (TIC), como el computador personal, telefonía móvil, banda ancha y otros dispositivos.

La Declaración de Principios adoptada por la Cumbre Mundial sobre la Sociedad de la Información, establece que los beneficios de la revolución de la tecnología y la información están actualmente distribuida de manera desigual entre los países desarrollados y en desarrollo y dentro de las sociedades. Esta declaración también incluye el compromiso de transformar esta brecha digital en una oportunidad digital para todos en

particular para aquellos que corren el riesgo de quedar rezagados y marginados.

Tomando en cuenta las brechas que El Salvador tiene en tecnologías de la información, no resulta fuera de la realidad que no se cuente en el país con peritos especializados en la rama de la informática, razón por la cual la investigación de los delitos informáticos recae sobre profesionales del peritaje que no están capacitados en las ramas de las tecnologías de la información.

En El Salador el Estado ha contado con el apoyo técnico y logístico de los Estados Unidos, para poder implementar el monitoreo de llamadas, correos electrónicos, y todo lo que está inmerso dentro del espectro electromagnético de comunicaciones, con la creación del centro de intervención a las telecomunicaciones.

La falta de infraestructura, herramientas modernas y demás implementos tecnológicos requeridos para la persecución de este tipo de delitos incrementa el riesgo de que la investigación sea realizada de una manera inadecuada por parte de los especialistas.

2.6 DESAFÍOS INVESTIGATIVOS Y PROCESALES DEL SISTEMA PENAL PARA LA APLICACIÓN DE LA LECDIC

En el año 2016 la normativa que busca proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación (TIC) en El Salvador.

2.6.1 Los principales retos para la aplicación de la ley

Lograr los consensos requeridos para la adecuada aplicación de dicha ley y lograr lo que su espíritu busca, que es prevenir los delitos informáticos, no sería ningún problema si no dependiera de la voluntad de los partidos políticos y de las instituciones a cargo de velar por su

aplicación, por ello, llegar consensos y promover los cambios requeridos se vuelven verdaderos retos.

El primero, es la reforma del CPP para que se integren las evidencias digitales dentro de su texto, la preservación y el tratamiento de dicha evidencia exige de mayor conocimiento sobre el funcionamiento de los objetos electrónicos que forman parte de un equipo computacional y de otros accesorios y equipos que se pueden conectar a él. En la reforma del CPP, debe especificarse el tratamiento de las evidencias digitales, pero también debe clarificar el accionar del perito informático.

Al tratarse de métodos y técnicas para extraer evidencias muy distintas a las que se emplean para las evidencias físicas, debe definirse cuáles pueden ser considerados como válidos. Otra actualización necesaria es sobre la cadena de custodia de la evidencia digital, que tiene otros aspectos técnicos más específicos y que deben ser incorporados a la cadena de custodia que se emplea para las otras evidencias ya reguladas en el Código.

Un segundo reto, es asegurar que tanto la FGR, PNC y CSJ cuenten con los recursos necesarios para aplicar la ley. Se conoce que la PNC tiene una Unidad de Delitos Informáticos, sin embargo dicha unidad apenas cuenta con el personal idóneo para ejercer las actividades mínimas que exige la aplicación de la ley. Además, se conoce que dicha unidad no cuenta con los materiales y equipos adecuados para la incautación de evidencias digitales en escenas de crimen informáticos.

El tercer se considera que está relacionado con la creación de metodologías, manuales y guías para el adecuado tratamiento de las evidencias digitales y su cadena de custodia. En los países que llevan más bagaje con leyes similares, se han creado documentos donde las principales instituciones encargadas de aplicar la ley, se coordinan para crear guías y manuales que contienen métodos, metodologías y técnicas

basadas en normas internacionales que son aplicadas como buenas prácticas, todo ello para garantizar la aplicación adecuada de la ley y evitar al máximo que los procesos judiciales se vean afectados por acciones inadecuadas.

2.6.2 El principal desafío

La LECDIC busca proteger los siguientes bienes jurídicos: “la información que garantice y proteja el ejercicio de derechos, fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros”.

La mencionada ley busca prevenir la comisión de delitos que se realicen con las Tecnologías de la Información y la Comunicación, pero para lograr su cometido se requiere que el Estado juegue un papel determinante; uno de ellos es sin duda la educación, el uso cada vez más intensivo de las TIC facilita también el cometimiento de los mismos. Un simple acto de interceptar una clave del router WiFi del vecino, convierte al hechor en un delincuente, no obstante, el desconocimiento de la ley hace que esta práctica se siga realizando.

CAPITULO III

PRESENTACIÓN, DESCRIPCIÓN E INTERPRETACIÓN DE RESULTADOS

PARTE I

3.1 RESULTADOS DE LA ENTREVISTA SEMI-ESTRUCTURADA

En este capítulo se desarrollara el análisis e interpretación del instrumento utilizado en la investigación de campo, dentro de la cual se encuentran la entrevista semi-estructurada, realizada a funcionarios y personas que tienen conocimientos sobre los delitos informáticos.

3.1.1 Descripción de la entrevista semi-estructurada

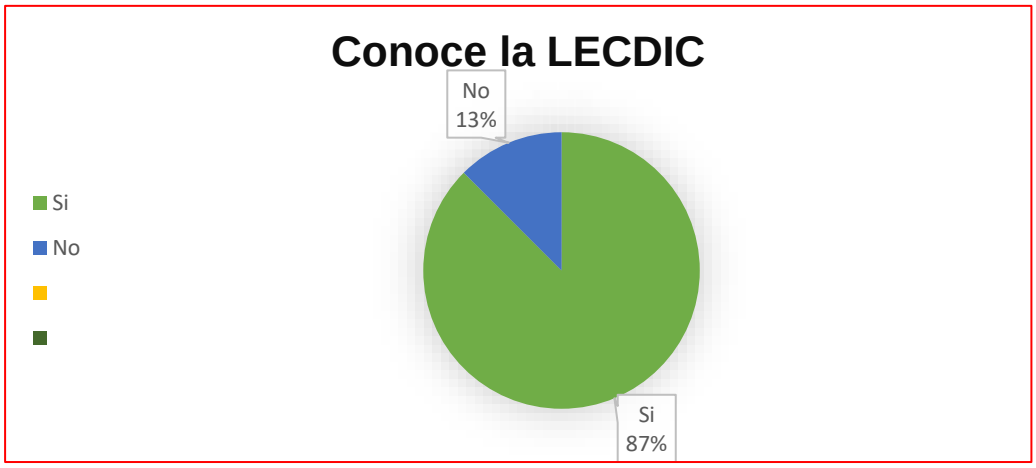
Con la realización de la entrevista en esta etapa de la investigación se ha pretendido conocer el punto de vista que tienen los diferentes funcionarios y personas conocedoras en el tema, y de esta manera obtener hacer un análisis comparativo entre las respuestas dadas por ellos.

El referido instrumento se realizó con la finalidad de conocer la perspectiva que tienen las personas entrevistadas sobre el objeto de estudio de la investigación para posteriormente evaluar en qué medida sustenta o no la investigación.

Pregunta Nº 1.

¿Conoce usted la Ley Especial Contra Delitos Informáticos y Conexos?

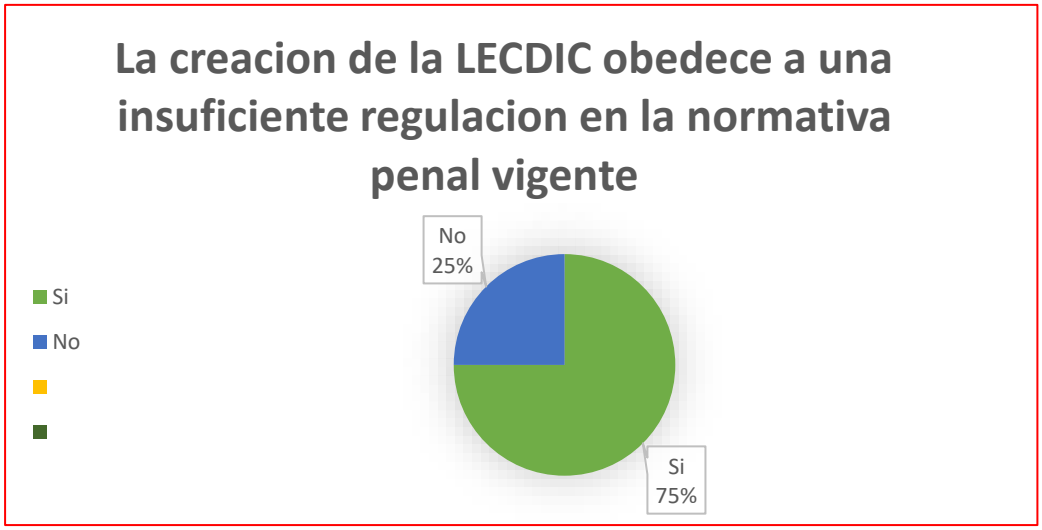
Opciones	fa	Fr%	fa	Fr%	Total
Si	7	87.5%			
No			1	12.5%	
Total	7	87.5%	1	12.5%	100%



Pregunta Nº 2.

¿Considera usted que la creación de la LECDIC obedece a una insuficiente regulación en la normativa penal vigente salvadoreña?.

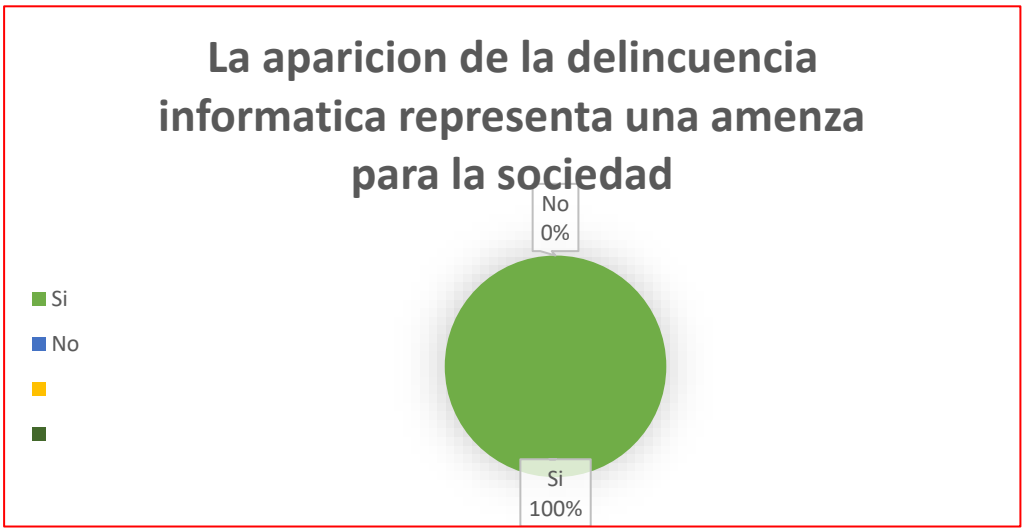
Opciones	fa	Fr%	fa	Fr%	Total
Si	6	75%			
No			2	25%	
Total	6	75%	2	25%	100%



Pregunta Nº 3.

¿Cree usted que usted que la aparición de un tipo de delincuencia ligada a las nuevas tecnologías representa para la sociedad civil una amenaza latente?

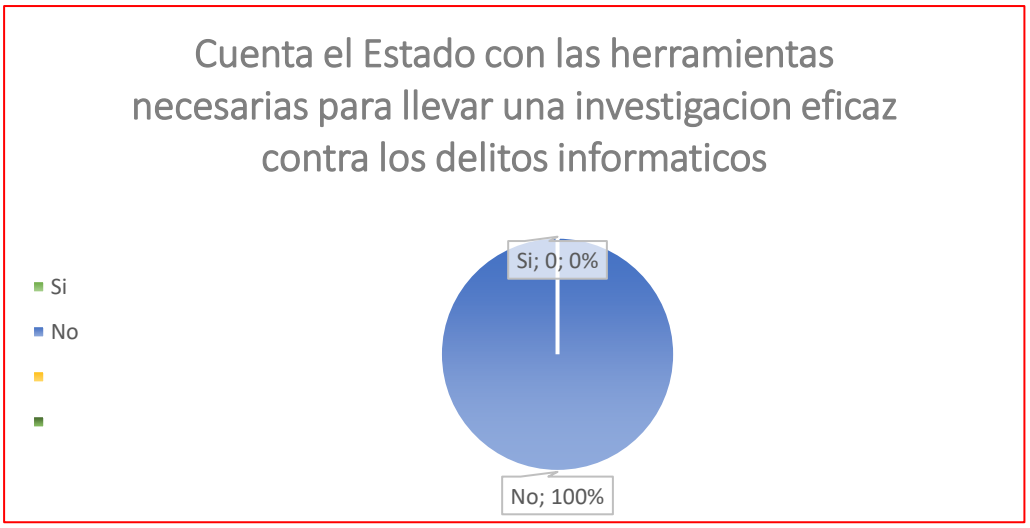
Opciones	fa	Fr%	fa	Fr%	Total
Si	8	100%			
No			0	0.0%	
Total	8	100%	0	0.0%	100%



Pregunta Nº 4.

¿Considera usted que el Estado cuenta con las herramientas necesarias para llevar a cabo una investigación efectiva contra los delitos informáticos y conexo?

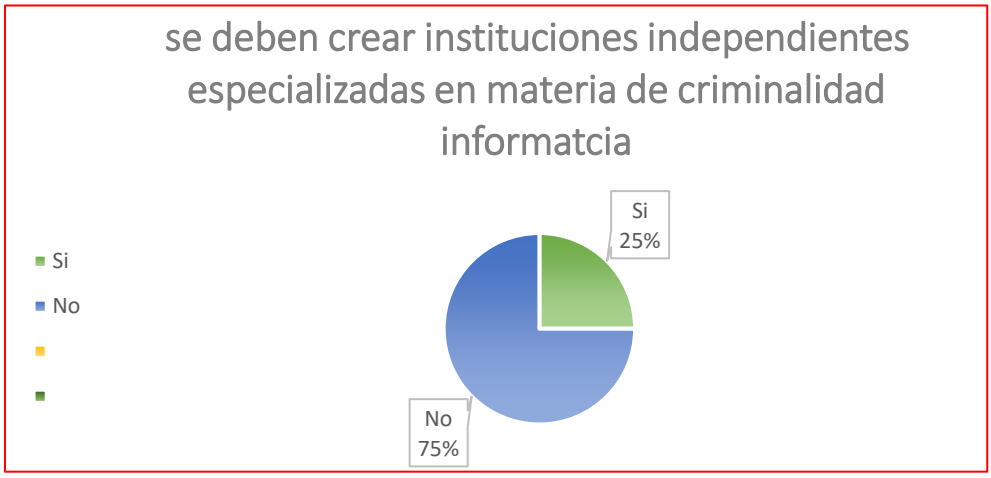
Opciones	fa	Fr%	fa	Fr%	Total
Si	0	0.0%			
No			8	100%	
Total	0	0.0%	8	100%	100%



Pregunta Nº 5.

¿Considera usted que se deben crear instituciones independientes especializadas en materia de criminalidad informática?

Opciones	fa	Fr%	fa	Fr%	Total
Si	2	25%			
No			6	75%	
Total	2	25%	6	75%	100%



FISCALIA GENERAL DE LA REPUBLICA

Código de la unidad de análisis	Código de pregunta	Tema fundamental	Categoría de enfoque	conclusión
01	06	La criminalidad informática posterior a la vigencia de la LECDIC.	Bajo el nombre de Ley Especial de Delitos Informáticos y Conexos, fue aprobada el 4 de febrero del año 2016 la normativa que busca proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación (TIC) en El Salvador.	Para el Ministerio Publico Fiscal, la criminalidad informática posterior a la vigencia de la LECDIC ha aumentado en gran medida.
	07	Los delitos informáticos más comunes que se cometen en El Salvador.	La proliferación de internet ha permitido el desarrollo de nuevos modus operandi para la ejecución de actividades criminales como difamación, amenaza, estafa,	En lo que respecta a la jurisdicción de San Miguel se ha anunciado con mayor frecuencia la revelación indebida de datos o información de carácter personal, estafa informática, acoso a través de la tecnología de la información

			violación a derechos de autor, distribución de pornografía. Infantil, robo de identidad, entre otras.	y comunicación, pornografía y Hurto de identidad.
	08	Las técnicas de investigación del Sistema Penal en la persecución de los delitos informáticos	Las técnicas de investigación en la persecución de la criminalidad informática requieren de técnicas especiales mediante la tecnología adecuada y de personal preparado para la averiguación del delito.	El proceso investigativo en los delitos informáticos permite la aplicación de todas las diligencias reguladas en el Código Procesal Penal, así como los diversos actos urgentes de comprobación. Sin embargo hay diferencias sustanciales de los delitos informáticos y los demás delitos en relación con las evidencias.
	09	Limitantes de la FGR para investigar los delitos informáticos.	Falta de preparación o capacitación por parte de la FGR que estén relacionados con los delitos informáticos.	No se cuenta con investigadores capacitados acorde al área informática, falta de conocimiento de algunos jueces con respecto al tratamiento de este tipo de delitos, así, la falta de equipo informático para el tratamiento adecuado.

	10	La ausencia de herramientas tecnológicas como limitante para investigar la criminalidad informática.	Falta de infraestructura y tecnología adecuada en los entes u organismos de investigación como: el Ministerio de Justicia y Seguridad Publica, la Policía Nacional Civil y la Fiscalía General de la Republica.	La ausencia de herramientas es una de las principales limitantes, por el hecho de que en su mayor proporción las evidencias con las que se cuentan para probar su existencia son digitales, y al no contar con herramientas idóneas obstaculizan en mayor proporción tener una buena investigación del hecho delictivo.
	11	La cooperación y colaboración internacional para una investigación y persecución penal exitosa.	Dada la dificultad que pueden encontrarse a la hora de resolver delitos informáticos, es necesario para los países ponerse de acuerdo con el objetivo de combatir los delitos informáticos de forma Efectiva.	Una buena Investigación depende en gran medida de una cooperación y colaboración internacional.
	12	Los principales retos para la aplicación de la LECDIC.	Lograr los consensos requeridos para la adecuada aplicación de dicha ley y lograr lo que su espíritu busca, que es prevenir los delitos informáticos.	Divulgación constante a la población de su existencia y aplicación, capacitación constante al sector de jueces o al gremio judicial, policías y fiscales.

JUEZ EJECUCION DE MEDIDAS SAN MIGUEL

Código de la unidad de análisis	Código de pregunta	Tema fundamental	Categoría de enfoque	conclusión
02	06	La criminalidad informática posterior a la vigencia de la LECDIC.	Bajo el nombre de Ley Especial de Delitos Informáticos y Conexos, fue aprobada el 4 de febrero del año 2016 la normativa que busca proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación (TIC) en El Salvador.	El Juez de Ejecución considera que si ha disminuido la criminalidad informática y que está logrando eficacia la normativa especial.
	07	Procesamiento de delitos regulados en la LECDIC.	Una suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial y de los jueces, el procesamiento de los delitos informáticos sería más eficaz.	Cuatro casos de delitos informáticos he procesado.

	08	Criterios para dictar una resolución en un proceso de delitos informáticos.	Los elementos esenciales que componen el debido proceso, se encuentran la motivación, fundamentación, congruencia y pertinencia entre otros, que deben ser observados por los juzgadores al momento de dictaminar sus resoluciones.	Que se logre establecer la participación de los imputados.
	12	Los principales retos para la aplicación de la LECDIC.	Lograr los consensos requeridos para la adecuada aplicación de dicha ley y lograr lo que su espíritu busca, que es prevenir los delitos informáticos.	Lograr que los habitantes de El Salvador conozcan de la LECDIC, a efecto de que alguna conducta no quede impune.

POLICIA NACIONAL CIVIL SAN MIGUEL.

Código de la unidad de análisis	Código de pregunta	Tema fundamental	Categoría de enfoque	conclusión
03	05	La criminalidad informática posterior a la vigencia de la LECDIC.	Bajo el nombre de Ley Especial de Delitos Informáticos y Conexos, fue aprobada el 4 de febrero del año 2016 la normativa que busca proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación (TIC) en El Salvador.	Para la Policía Nacional Civil, la criminalidad informática posterior a la vigencia de la LECDIC ha aumentado.
	06	Los delitos informáticos más comunes que se cometen en El Salvador.	La proliferación de internet ha permitido el desarrollo de nuevos modus operandi para la ejecución de actividades criminales.	Los delitos informáticos más comunes son la Revelación Indebida de Datos e Información de Carácter Personal, Pornografía.
	07	Los delitos complejos para el	La investigación de la delincuencia informática, no es una tarea fácil, ya	Los delitos más complejos para investigar en el Departamento de San

		proceso investigativo regulados en la LECDIC.	que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales que de acuerdo a sus características suelen ser volátiles y de vida corta.	Miguel son: la pornografía, acoso, divulgación de imágenes por medio de Facebook.
	08	Limitantes de la PNC para investigar los delitos informáticos.	Falta de preparación o capacitación por parte de la PNC que estén relacionados con la investigación de los delitos informáticos.	Muchas empresas internacionales no están obligadas a dar información, porque para El Salvador es delito para otros países no lo son, falta de capacitación del personal PNC, no invierten en tecnología.
	10	La ausencia de herramientas tecnológicas como limitante para investigar la criminalidad informática.	Falta de la infraestructura y tecnologías adecuada en los entes u organismos de investigación como: el Ministerio de Justicia y Seguridad Publica, la Policía Nacional Civil y la Fiscalía General de la Republica.	Si la falta de infraestructura es una de las principales limitantes; más que todo debería invertir tanto en compra de computadoras de amplia gama como licencias de programas y sistemas.

	11	La cooperación y colaboración internacional para una investigación y persecución penal exitosa.	Dada la dificultad que pueden encontrarse a la hora de resolver delitos informáticos, es necesario para los países ponerse de acuerdo con el objetivo de combatir los delitos informáticos de forma Efectiva.	Una buena Investigación depende en gran medida de una cooperación y colaboración internacional.
	12	Los principales retos para la aplicación de la LECDIC.	Lograr los consensos requeridos para la adecuada aplicación de dicha ley y lograr lo que su espíritu busca, que es prevenir los delitos informáticos.	**-** capacitación en delitos informáticos, tanto en Jueces, FGR, PNC. **-** Aportarle al peritaje informático **-** Invertir en tecnología para el combate de la criminalidad informática. **-** Asocio con empresas Internacionales que brindan la tecnología llámese Facebook, whatsapp etc.

PARTE II.

3.2 INFORME FINAL DE LA INVESTIGACION

3.2.1 PROBLEMAS DE LA INVESTIGACIÓN. VALORACIONES DE SOLUCIONES

1. **¿Cuáles son las dificultades que presenta el sistema penal salvadoreño al momento de la aplicación de la ley especial contra los delitos informáticos y conexos?**

La criminalidad informática en El Salvador se encuentra con limitantes a la hora de aplicar la LECDIC, en donde la investigación no es una tarea fácil, la mayoría de los datos probatorios son intangibles y transitorios, los vestigios digitales que de acuerdo a sus características suelen ser volátiles y de vida corta. La falta de infraestructura y la tecnología adecuada en los entes u organismos de investigación son una de las principales dificultades para que la ley sea eficaz. (Capitulo II, 2.4 Limitaciones del sistema penal para la investigación de los delitos informáticos.)

2. **¿Cuál es el proceso correspondiente para una efectiva tramitación de los delitos informáticos?**

El proceso investigativo en los delitos informáticos permite la aplicación de todas las diligencias reguladas en el CPP, así como los diversos actos urgentes de comprobación, Sin embargo, deben estimarse las diferencias sustanciales de los delitos informáticos y los demás delitos, en relación con las evidencias, mientras en los delitos tradicionales la evidencia generalmente cuenta con un carácter material o corpóreo, las evidencias digitales carecen de él, y se mantienen dentro de soportes que los contienen, pero que no los sustituyen sino que sólo los soportan. (Capitulo II, 2.3 el proceso investigativo de los delitos informáticos.)

3. **¿Cuáles son las técnicas de investigación con las que cuenta el sistema penal salvadoreño en la persecución de los delitos informáticos?**

Las investigación en la persecución de la criminalidad informática requieren de técnicas especiales mediante la tecnología adecuada y de personal preparado para la averiguación del delito; el proceso investigativo permite la aplicación de todas las diligencias reguladas en el CPP, así como los diversos actos urgentes de comprobación. Sin embargo, hay diferencias sustanciales entre los delitos informáticos y los demás delitos en relación con las evidencias. (Capitulo III, Parte I: Entrevista Semi-Estructurada)

4. **¿Qué criterios deben considerar los aplicadores del derecho al momento de dictar una resolución en un proceso referente a los delitos informáticos para el acceso a la justicia?**

Los elementos esenciales que componen el debido proceso se encuentran la motivación, fundamentación, congruencia y pertinencia entre otros, que deben ser observada por los juzgadores al momento de dictaminar sus resoluciones y establecer la participación del imputado en cualquier caso concreto respecto a los delitos informáticos. (Capitulo III, Parte I: Entrevista Semi-Estructurada).

3.2.2 LOGRO DE OBJETIVOS

OBJETIVO GENERAL.

1. **Identificar las dificultades que presenta el sistema penal salvadoreño al momento de la aplicación y tramitación de un proceso de delitos informáticos, y determinar en qué medida esta ley representa una garantía.**

Las dificultades para la tramitación del proceso de un delito regulado en la LECDIC por parte del sistema penal se desarrollaron en el “Capítulo

II, 2.4 limitaciones del sistema penal para la investigación de los delitos informáticos"; dentro las cuales se encuentran las limitaciones de infraestructura, limitaciones tecnológicas, limitaciones de formación. Tomando en cuenta las brechas que El Salvador tiene en tecnologías de la información, no se cuenta en el país con peritos especializados en la rama de la informática, razón por la cual la investigación de los delitos informáticos recae sobre profesionales del peritaje que no están capacitados en las ramas de las tecnologías de la información.

OBJETIVO ESPECIFICO 1.

1. **Analizar los procedimientos correspondientes a seguir en la tramitación de los delitos informáticos.**

El procedimiento de tramitación de los delitos informáticos se comprobó que sigue la misma línea de un procedimiento común regulado en el CPP; mediante el desarrollo del "Capítulo II, 2.3 limitaciones del sistema penal para la investigación de los delitos informáticos"; él se identifica que por no contar con un procedimiento especial deben estimarse la diferencias sustanciales de los delitos informáticos y los demás delitos, en relación con las evidencias, mientras en los delitos tradicionales la evidencia generalmente cuenta con un carácter material o corpóreo, las evidencias digitales carecen de él.

OBJETIVO ESPECIFICO 2.

2. **Determinar las técnicas de investigación con las que cuenta el sistema penal salvadoreño en la persecución de los delitos informáticos.**

Las técnicas que utiliza el sistema penal salvadoreño para la persecución de los delitos informáticos se desarrolló en el "Capítulo III. 3.1 resultados de la entrevista semi-estructurada"; mediante la entrevista semi-estructurada a los especialistas y conocedores del tema de

investigación, lo cual manifestaron que no se cuentan con técnicas especiales para la aplicación de la LECDIC, es decir, con la tecnología adecuada y el personal preparado para la averiguación del delito, para una aplicación eficaz de la ley.

OBJETIVO ESPECIFICO 3.

3. **Examinar cada uno de los criterios a tomar en cuenta por parte de los aplicadores del derecho al encontrarse frente a las deficiencias de investigación en un proceso de delitos informáticos.**

Los criterios que deben tomarse en cuenta para dictar una resolución en cada caso concreto de los delitos informáticos regulados en la LECDIC se desarrolló en el “Capítulo III. 3.1 resultados de la entrevista semi-estructurada”, realizada a los especialistas y conocedores del tema de investigación; los criterios son los mismos regulados para los delitos tradicionales, es decir, motivación, fundamentación, congruencia y pertinencia entre otros, que deben ser observada por los juzgadores al momento de dictaminar sus resoluciones y establecer la participación del imputado.

3.2.3 HIPÓTESIS DE LA INVESTIGACIÓN. VERIFICACIÓN Y DEMOSTRACIÓN

HIPOTESIS GENERAL

Frente al inminente avance de las tecnologías y el uso indebido de estas, el sistema penal salvadoreño se vio en la necesidad de la creación de la ley especial contra los delitos informáticos y conexos, como garante del sistema informático y datos personales, sin embargo en la practica el sistema penal podría presentar diferentes desafíos para la correcta aplicación de la ley.

La LECDIC fue aprobada el 4 de febrero del año 2016, la normativa que busca proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación (TIC) en El Salvador; no obstante en la práctica tiene muchas limitantes para una proceso vigoroso en la investigación del delito. Mediante el desarrollo del capítulo III, se demuestra los desafíos investigativos y procesales que el sistema penal debe de aplicar para que la ley se vuelva eficaz.

HIPOTESIS ESPECIFICA 1.

El proceso común es totalmente eficaz dentro del sistema penal salvadoreño frente a las exigencias de la ley especial contra los delitos informáticos y conexos.

La verificación de esta hipótesis se ha cumplido en el desarrollo del Capítulo II, en donde se establece que el proceso investigativo de los delitos informáticos permite la aplicación de todas las diligencias reguladas en el CPP, así como los diversos actos urgentes de comprobación; sin embargo por no tener un proceso especial la investigación del delito informático carece de ciertos elementos que ayudarían a probar la existencia del delito, como es el caso de las evidencias digitales que no están incorporadas en el CPP.

HIPÓTESIS ESPECIFICA 2.

La falta de herramientas específicas para la persecución de los delitos informáticos vuelve ineficaz la LEDIC.

La verificación de esta hipótesis se ha cumplido en el desarrollo del capítulo III, mediante la realización de la entrevista semi-estructurada, en donde los especialistas manifestaron que no se cuentan con técnicas especiales para la aplicación de la LECDIC, es decir, con la tecnología adecuada y el personal preparado para la averiguación del delito; en

relación con el desarrollo del capítulo II, el proceso investigativo de los delitos informáticos, donde queda en evidencia que el peritaje debe de tener conocimientos especiales para el manejo de las evidencias.

HIPÓTESIS ESPECIFICA 3.

Si bien es cierto, los delitos informáticos se encuentran regulados en una ley especial, como garantía del sistema informático, sin embargo, al no contar la FGR y la PNC con las herramientas y conocimientos en el ejercicio práctico, esta ley perdería su objetivo como garante de la seguridad de la informática.

La verificación de esta hipótesis se ha cumplido en el desarrollo de la entrevista semi-estructurada, en donde no todo las personas encargadas de administrar justicia conocían a profundidad de la aplicación de la LECDIC, debido a la falta de preparación a nivel de formación en el ámbito de los procedimientos y técnicas utilizadas para la persecución de los delitos informáticos, es decir, el Ministerio de Justicia y Seguridad Publica, la Policía Nacional Civil, jueces no cuentan con los recursos y capacitaciones necesarias por parte del Estado para la adecuada aplicación de la ley.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

4.1.1 Conclusiones Generales

Conclusiones Doctrinales

- El acceso a internet puede ser considerado un indicador de desarrollo, así como una ventana de oportunidad, esto no es siempre el caso, las tecnologías de la información a pesar que producen cambios de desarrollo también pueden utilizarse, para perpetrar y facilitar diversas actividades delictivas en manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público.
- La marcha de la informática genera, por un lado, enormes ventajas, pero por otro lado plantea problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informático, es decir, el desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables, y a medida que haya adelantos en ella, aumentará progresivamente la amenaza dañina.

Conclusiones Jurídicas

- El constante avance tecnológico y las nuevas formas de comisión de delitos, no deben estar separadas de las correspondientes reformas y creaciones legales, se deben crear nuevas normas que abarquen y contemplen las posibles vulneraciones a los derechos constitucionales para que las personas puedan tener opciones y medios dónde acudir para denunciar y protegerse frente a cualquier delito informático.

- Penalizar conductas antisociales, realizadas a través del uso de recursos informáticos, es una exigencia del desarrollo social, en El Salvador, el derecho penal y el derecho en su conjunto deben marcar límites en la conducta de los operadores de sistemas informáticos, mediante la tipificación penal de los comportamientos antisociales que pueden derivarse del uso de medios electrónicos. La revolución digital, como todas las revoluciones, genera incertidumbre pero lo importante es saber responder rápidamente a las exigencias de la vida social, de esto dependerá el futuro del país. Una ley especial (LECDIC) es el primer paso de un proyecto de amplio alcance para colocar a El Salvador a la par de los países desarrollados.

Conclusiones Socioeconómicas

- La Era Digital y la Sociedad de la Información han provocado un cambio de paradigma social y cultural, impactando drásticamente en la estructura socio – económica, provocando una reestructura de los negocios e industria. Sin la informática las sociedades actuales colapsarían, pues es un instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva de forma de energía, e inclusive, de poder intelectual; por lo que se puede decir que paralelamente al avance tecnológico, hay un avance más desarrollado en el delincuente, ya que este, tiene que tener un amplio conocimiento de estos avances tecnológicos, los cuales, no los ocupan en realizar el bien sino para delinquir.
- Con los avances tecnológicos en El Salvador tiene sus efectos en la comercialización electrónica, donde emplean esos medios informáticos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y

afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo.

4.1.2 Conclusiones Específicas

- El Salvador está intentando dar sus primeros pasos en el desarrollo de iniciativas que permitan la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesiones dedicados a su investigación.
- Paralelamente al avance tecnológico, hay un avance más desarrollado en el delincuente, ya que este, tiene que tener un amplio conocimiento de estos avances tecnológicos, los cuales, no los ocupan en realizar el bien sino para delinquir.
- Debido a la falta de una correcto conocimiento en los operadores de justicia como lo son los policías, fiscales, jueces así como todos aquellos que están involucrados en el que hacer en desarrollo de los procesos judiciales, y que son los encargados de que este tipo actividades delincuenciales puedan ser ventilados en los tribunales y con ello se logre una protección a todas aquellas personas que hacen uso de las estas herramientas tecnológicas.

4.2 RECOMENDACIONES

Al Estado de El Salvador (Órgano Ejecutivo)

- Para la implementación e investigación de estos tipos de delitos se debe mejorar la coordinación y el trabajo conjunto entre los organismos involucrados en la adopción de medidas de seguridad de la información como son Policías, Organismos judiciales entre otros.

- Concientizar sobre el problema y dar a conocer las medidas preventivas, para una política integral contra los delitos informáticos, elaborar un diagnóstico amplio de la situación de la infraestructura informática nacional implementando los mecanismos que permitan que dichas investigaciones se realicen con la tecnología y personal adecuada.
- Desarrollar contenidos y programas de formación de profesionales especialistas en seguridad de la información, que la aborden desde distintas visiones: técnica, legal y educación.
- Incentivar mecanismos de cooperación con otros países con el objetivo de prevenir y sancionar el delito informático que traspasa las fronteras de las naciones.

Al Órgano Judicial

- Desarrollo de programas de capacitación al órgano judicial (Fiscales, Jueces, Policía Nacional Civil) sobre los delitos informáticos y la informática legal, como Capacitación de tecnología en aspectos básicos de informática legal, forense, criminalística, manejo de evidencias digitales, etc.
- Asegurar que tanto la FGR, PNC y CSJ cuenten con los recursos necesarios para aplicar la ley y la creación de más Unidades de Delitos Informáticos con el personal idóneo.

A los Diputados de la Asamblea Legislativa

- Una reforma del Código Procesal Penal para que se integren las evidencias digitales dentro de su texto, la preservación y el tratamiento de dicha evidencia exige de mayor conocimiento sobre el funcionamiento de los objetos electrónicos que forman parte de un equipo computacional y de otros accesorios y equipos que se pueden conectar a él.

A La Sociedad.

- Inducirlos a través de campañas de concientización a Adoptar una actitud responsable frente al uso de las tecnologías de información, capacitándose para minimizar los riesgos que las acompañan.
- Denunciar los incidentes de seguridad ante las instancias que correspondan, permitiendo su seguimiento y contribuyendo así a su resolución.

BIBLIOGRAFIA

LIBROS

1.- BAÓN RAMÍREZ, R. (1996) “Visión general de la informática en el nuevo Código Penal”, en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid.

2.- Callegeri, N. (1985). "Delitos informáticos y legislación" en Revista de la facultad de derecho y ciencias políticas de la Universidad de Pontificia Bolivariana. Medellín, Colombia.

4.- Camacho, Losa, L. (1987). El Delito Informático. Madrid España: Civitas.

5.- Carrasco, L. (2010). "Casos de Suplantación de Identidad Detectados en Denuncias Tramitadas por la Agencia Española de Protección de Datos" citado por Marta y Martin, Ricardo en " El robo de Identidad". España: Universidad de Castilla.

6.- Climent, Barrera, J. (2001). Conferencia la Justicia Penal en Internet. Territorialidad y competencias penales, Consejo General del Poder Judicial (pág. 75). Estados Unidos: Biblioteca Judicial Fernando Coto.

7.- Creus, C. (2004). "Derecho Penal, Parte General". Buenos Aires, Argentina: Editorial Buenos Aires.

8.- Davara Rodríguez, M. A. (1990). Análisis de la Ley de Fraude Informático, Revista de Derecho. San Salvador: UNAM.

9.- Devoto, M. (2001). Comercio Electrónico y firma digital: las regulaciones del ciberespacio y las estrategias globales. Buenos Aires, Argentina: La Ley S.A., primera edición.

10.- Fernández Calvo, R. (1996). El Tratamiento del llamado "Delito Informático" en el proyecto de Ley Orgánica del Código Penal: Reflexiones y propuestas de la GLI. Mérida: UNED.

11.- GÓMEZ PERALS, M. (1994) “Los Delitos Informáticos en el Derecho Español”. España: Editorial Aranzadi Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25.

12.- Harb, M. B. (2003). Derecho Penal. La Paz, Bolivia: Editorial Juventud.

13.- Herman Hollerith, B. (1895). Pionero de la informática por su invención de las maquinas estadísticas de tarjetas o fichas perforadas. Estados Unidos.

14.- Huerta Miranda, M. &. (19990). Los Delitos Informáticos. España: Cono Sur.

15.- Jiménez Castillo, M. (1989). El Delito Informático, Congreso Sobre Derecho Informático. Zaragoza, España: Civitas.

16.- Landaverde Contreras, M. &. (2000). Delitos Informáticos. San Salvador: Universidad de El Salvador.

17.- López Ortega, J. J. (2001). Conferencia Libertad de expresión y responsabilidad por contenidos en internet. Consejo General del Poder Judicial (pág. 75). Estados Unidos: Biblioteca Judicial Fernando Coto.

18.- Magliona, Markovicth, C. P., & & López Medel. (1999). Delincuencia y Fraude Informático. Chile: Editorial Jurídica.

19.- Mata, R. M. (2003). Delincuencia Informática y Derecho penal. México: Híspame.

20.- Mohrenschlager, M. (1992). El Nuevo Derecho Penal Informático. Alemania: Cono Sur.

21.- Núñez, R. (1987). "Manual de Derecho Penal". Córdoba: Editorial Heliasta.

22.- Omero Flores, R. (2016). "Las Conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa". México: Unam.

23.- Pardini, A. A. (2002). Derecho de Internet. Buenos Aires, Argentina: La Rocca.

24.- Reyes Echandia, A. (1981). La Tipicidad. Colombia: Universidad de Externado.

25.- Rivas, J. (2012). Historia de la Computación. El Salvador: Comunicaciones Informáticas.

26.- Rodríguez, Martínez, L. J. (2001). Conferencia: los virus informáticos y el delito de daños. Consejo General del Poder Judicial (pág. 75). Estados Unidos: Biblioteca Judicial Fernando Coto.

27.- Romeo Casanova, C. (2003). Poder Informático y Seguridad Jurídica. España: civetas.

28.- Rovira Canto, E. (2002). Delincuencia Informática y Fraudes Informáticos. Granada: Comares.

29.- Téllez, Valdés, J. (1996). "Los Delitos Informáticos". México: 1º Edición.

30.- Tiedemann, K. (1985). El Poder Informático. Barcelona, España: Civitas.

31.- UNODOC. (2016). Dirección General de Estadísticas y Censos, Ministerio de Economía: Estimaciones y Proyecciones de Población Nacional 2005-2050. San Salvador: Cybercrime.

32.- UNODOC. (2016). La Droga y el Delito. El Salvador: Oficina de Naciones Unidas, Documentos Internos.

SITIO WEB

1.- Chavarría, A. R. (12 de 06 de 2016). Delitos Informáticos. Obtenido de Legislación y manejo de la Información: www.ictparliamet.org/sites/default/files/delitosinformaaticos

2.- Colveo, J. L. (13 de octubre de 2017). Los Nombres de Dominio. Obtenido de Anetcom Generalitat: https://www.filmac.com/wp-conten/uploads/librodominios

3.- De Pino, S. A. (18 de 06 de 2016). Delitos Informáticos. Obtenido de Generalidades: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.

4.- Rodríguez, V. M. (marzo de 2017). Análisis de la Ley de Delitos Informáticos. Obtenido de Policía Nacional Civil, Subdirecciones de Investigaciones: Sitio Web: www.unodoc.org./Ropan.

5.- Superintendencia General de Electricidad, T. (23 de marzo de 2013). https://www.siget.gob.sv/temas/telecomunicaciones/estadistica/boletin-estadistico/. Obtenido de Boletín Estadístico de Telecomunicaciones: https://www.siget.gob.sv/temas/telecomunicaciones/estadistica/boletin-estadistico/.

LEGISLACION INTERNACIONAL

1.- Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest) Sesión N°109, celebrada el 8 de noviembre de 2001, presentado para su firma en la ciudad de Budapest, con fecha 23 de noviembre de 2001, entrando en vigencia el 1 de julio de 20041

LEGISLACION NACIONAL

1.- Constitución de la República de El Salvador, Decreto No. 38, Diario Oficial No. 234, Tomo 281, San Salvador, El Salvador, 1983.

2.- Ley Especial Contra Delitos Informáticos y Conexos, Decreto Nº 260, D.O. Nº 40, Tomo Nº 410, El Salvador 2016.

3.- Código Penal, Decreto Nº 1030. D. O. N° 105 Tomo N° 335. Fecha: 10 de junio de 1997.

4.- Código Procesal Penal, Decreto No. 904, Diario Oficial No. 11, Tomo 334, El Salvador, 1998.

ANEXOS

ANEXO 1. ENTREVISTA SEMI-ESTRUCTURADA

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

PROCESO DE GRADUACIÓN DE LICENCIATURA EN CIENCIAS JURÍDICAS

TEMA: DESAFÍOS DEL SISTEMA PENAL SALVADOREÑO EN LA APLICACIÓN DE LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS.

Entrevista semi-estructurada dirigida a Especialistas del Derecho Procesal Penal de El Salvador: *Fiscalía General de la Republica.*

Objetivo: Recabar información sobre las diferentes posturas en cuanto a la temática del desafíos del sistema penal salvadoreño en la aplicación de la LECDIC.

Indicación: Conteste las interrogantes que a continuación se le plantean según su conocimiento personal y convicción que tiene sobre el tema de investigación.

1- **¿Conoce usted la Ley Especial Contra Delitos Informáticos y Conexos?**

2- **Considera usted que la creación de la LECDIC obedece a una insuficiente regulación en la normativa penal vigente salvadoreña. Si, No. ¿Por qué?**

3- **Cree usted que usted que la aparición de un tipo de delincuencia ligada a las nuevas tecnologías representa para la sociedad civil una amenaza latente. Si, No. ¿Por qué?**

4- **Considera usted que el Estado cuenta con las herramientas necesarias para llevar a cabo una investigación efectiva contra los delitos informáticos y conexo. Si, No. ¿Por qué?**

5- **Considera usted que se deben crear instituciones independientes especializadas en materia de criminalidad informática. Si, No. ¿Por qué?**

6- **¿A su criterio, ha aumentado o disminuido la criminalidad informática, posterior a la vigencia de la LECDIC?**

7- **¿Cuáles son los delitos informáticos más comunes que se cometen en el salvador?**

8- **¿Cuáles son las técnicas de investigación con las que cuenta el sistema penal salvadoreño en la persecución de los delitos informáticos?**

9- **¿Cuáles son las limitantes con las que se encuentra la FGR a la hora de investigar los delitos informáticos y conexos?**

10- **Considera usted que una de las limitantes para investigar la criminalidad informática es la ausencia de las herramientas tecnológicas idóneas para investigar dichos delitos. Si, No. ¿Por qué?**

11- **¿Cree usted que para que haya una investigación y persecución penal exitosa, es indispensable una fuerte cooperación y colaboración internacional?**

12- **¿A su criterio cuáles son los principales retos para la aplicación de la LECDIC?**

ANEXO 2. ENTREVISTA SEMI-ESTRUCTURADA

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

PROCESO DE GRADUACIÓN DE LICENCIATURA EN CIENCIAS JURÍDICAS

TEMA: DESAFÍOS DEL SISTEMA PENAL SALVADOREÑO EN LA APLICACIÓN DE LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS.

Entrevista semi-estructurada dirigida a Especialistas del Derecho Procesal Penal de El Salvador: *Unidad de Delitos Especializados PNC.*

Objetivo: Recabar información sobre las diferentes posturas en cuanto a la temática del desafíos del sistema penal salvadoreño en la aplicación de la LECDIC.

Indicación: Conteste las interrogantes que a continuación se le plantean según su conocimiento personal y convicción que tiene sobre el tema de investigación.

1- **¿Conoce usted la Ley Especial Contra Delitos Informáticos y Conexos?**

2- **Considera usted que la creación de la LECDIC obedece a una insuficiente regulación en la normativa penal vigente salvadoreña. Si, No. ¿Por qué?**

3- **Cree usted que usted que la aparición de un tipo de delincuencia ligada a las nuevas tecnologías representa para la sociedad civil una amenaza latente. Si, No. ¿Por qué?**

4- **Considera usted que el Estado cuenta con las herramientas necesarias para llevar a cabo una investigación efectiva contra los delitos informáticos y conexo. Si, No. ¿Por qué?**

5- **¿A su criterio, ha aumentado o disminuido la criminalidad informática, posterior a la vigencia de la LECDIC?**

6- **¿Cuáles son los delitos informáticos más comunes que se cometen en el salvador?**

7- **A su criterio qué delito o delitos regulados en la LECDIC se le es más complejo para el proceso investigativo. ¿Por qué?**

8- **¿Cuáles son las técnicas de investigación con las que cuenta la Unidad de Delitos Especializados en la persecución de los delitos informáticos?**

9- **¿Cuáles son las limitantes con las que se encuentra la Unidad de Delitos Especializados a la hora de investigar los delitos informáticos y conexos?**

10- **Considera usted que una de las limitantes para investigar la criminalidad informática es la ausencia de las herramientas tecnológicas idóneas para investigar dichos delitos. Si, No. ¿Por qué?**

11- **¿A su criterio cuáles son los principales retos para la aplicación de la LECDIC?**

ANEXO 3. ENTREVISTA SEMI-ESTRUCTURADA

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

PROCESO DE GRADUACIÓN DE LICENCIATURA EN CIENCIAS JURÍDICAS

TEMA: DESAFÍOS DEL SISTEMA PENAL SALVADOREÑO EN LA APLICACIÓN DE LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS.

Entrevista semi-estructurada dirigida a Especialistas del Derecho Procesal Penal de El Salvador: *Jueces en el Área Penal.*

Objetivo: Recabar información sobre las diferentes posturas en cuanto a la temática del desafíos del sistema penal salvadoreño en la aplicación de la LECDIC.

Indicación: Conteste las interrogantes que a continuación se le plantean según su conocimiento personal y convicción que tiene sobre el tema de investigación.

1- **¿Conoce usted la Ley Especial Contra Delitos Informáticos y Conexos?**

2- **Considera usted que la creación de la LECDIC obedece a una insuficiente regulación en la normativa penal vigente salvadoreña. Si, No. ¿Por qué?**

3- **Cree usted que usted que la aparición de un tipo de delincuencia ligada a las nuevas tecnologías representa para la sociedad civil una amenaza latente. Si, No. ¿Por qué?**

4- **Considera usted que el Estado cuenta con las herramientas necesarias para llevar a cabo una investigación efectiva contra los delitos informáticos y conexo. Si, No. ¿Por qué?**

5- **Considera usted que se deben crear instituciones independientes especializadas en materia de criminalidad informática. Si, No. ¿Por qué?**

6- **A su criterio, aumentado o disminuido la criminalidad informática, posterior a la vigencia de la LECDIC?**

7- **Cuántos casos ha conocido de delitos regulados en la LECDIC?**

8- **¿Qué criterios deben considerar al momento de dictar una resolución en un proceso referente a los delitos informáticos?**

9- **¿A su criterio cuáles son los principales retos para la aplicación de la LECDIC?**

ANEXO 4. ENTREVISTA SEMI-ESTRUCTURADA

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE JURISPRUDENCIA Y CIENCIAS SOCIALES.

PROCESO DE GRADUACIÓN DE LICENCIATURA EN CIENCIAS JURÍDICAS

TEMA: DESAFÍOS DEL SISTEMA PENAL SALVADOREÑO EN LA APLICACIÓN DE LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS.

Entrevista semi-estructurada dirigida a Especialistas del Derecho Procesal Penal de El Salvador: *Abogados defensores: PGR/ Particulares.*

Objetivo: Recabar información sobre las diferentes posturas en cuanto a la temática del desafíos del sistema penal salvadoreño en la aplicación de la LECDIC.

Indicación: Conteste las interrogantes que a continuación se le plantean según su conocimiento personal y convicción que tiene sobre el tema de investigación.

1- **¿Conoce usted la Ley Especial Contra Delitos Informáticos y Conexos?**

2- **Considera usted que la creación de la LECDIC obedece a una insuficiente regulación en la normativa penal vigente salvadoreña sobre ese tipo de delitos. Si, No. ¿Por qué?**

3- **Cree usted que usted que la aparición de un tipo de delincuencia ligada a las nuevas tecnologías representa para la sociedad civil una amenaza latente. Si, No. ¿Por qué?**

4- **Considera usted que el Estado cuenta con las herramientas necesarias para llevar a cabo una investigación efectiva contra los delitos informáticos y conexo. Si, No. ¿Por qué?**

5- **Considera usted que se deben crear instituciones independientes especializadas en materia de criminalidad informática. Si, No. ¿Por qué?**

6- **¿Qué son Para usted los delitos informáticos y conexos?**

7- **¿A su criterio, ha aumentado o disminuido la criminalidad informática, posterior a la vigencia de la LECDIC?**

8- **¿Cuáles son los delitos informáticos más comunes que ha representado en un proceso penal?**

9- **¿Cuáles son las limitantes con las que se encuentra a la hora de ejercer el derecho de defensa referente a los delitos informáticos y conexos?**

10- **¿A su criterio cuáles son los principales retos para la aplicación de la LECDIC?**